Scope

This policy applies to all Indiana University School of Medicine (IUSM) Graduate Medical Education (GME) resident and fellow physicians.

Reason for Policy

The purpose of this policy is to provide guidelines for use of online social networks.

Policy Statement

Weblogs and online social networks have become popular communication tools over the past several years. These forums offer unique opportunities for people to interact and keep in contact, and have great potential to augment friendships and professional interactions. As professionals with a unique social contract and obligation, medical students, residents, as well as practicing physicians must be cognizant of the public nature of these forums and the permanent nature of posting therein. While these sites offer potential to bolster communications with friends and colleagues, they are also a potential forum for lapses of professionalism and professional behavior. These sites may give the impression of privacy, but postings and other data should be considered in the
public realm and freely visible by many people. IUSM has adopted the following guidelines to assist residents in safely and responsibly using these sites and applies to participation in social networks personally or professionally and with personal or IU computing equipment.

---

**Procedures**

The following lists guidelines for ethical and professional behavior.

**Professionalism**

(a) Postings within social network sites are subject to the same professionalism standards as any other personal interactions. The permanence and written nature of these postings make them even more subject to scrutiny than most other forms of communication. The professionalism description can be found in the IUSM honor code, which is signed by all students, residents, fellows and faculty. Residents may be subject to disciplinary actions within the school for comments that are either unprofessional or violate patient privacy.

(b) Statements made by you within online networks will be treated as if you verbally made the statement in a public place.

(c) Do not violate copyrighted or trademarked materials. If you post content, photos or other media, you are acknowledging that you own or have the right to use these items.

(d) In online social networks, the lines between public and private, personal and professional are blurred. Just by identifying yourself as an IUSM resident, you are creating perceptions about IUSM by those who have access to your social network profile or weblog. Be sure that all content associated with you is consistent with your position at the school and with IUSM’s values and professional standards.

(e) IU logos may not be used on any social media site without the approval of the IUSM Office of Strategic Communications. Any medically oriented weblogs should contain the disclaimer: “The posts on this site are my own and do not necessarily represent the IU School of Medicine’s positions, strategies, or opinions.”

(f) Use of these social networking sites or weblogs can have legal ramifications. Comments made regarding care of patients or that portray you or a colleague in an unprofessional manner can be used in court or other disciplinary proceedings (i.e. state medical licensing boards).

(g) Unprofessional postings by others on your page reflect very poorly on you. Please monitor others’ postings on your profile and work to ensure that the
content would not be viewed as unprofessional. It may be useful to block postings from individuals who post unprofessional content.

(h) Residents are encouraged to alert colleagues to unprofessional or potentially offensive comments made online to avoid future indiscretions and refer them to this document.

(i) Keep in mind that statements and photos posted within these sites are potentially viewable by future employers, and even if deleted can be recovered under certain circumstances. Be aware, too, that images can be downloaded by and forwarded to others. It is not uncommon for potential employers to search for the social network profiles of potential hires, and there are many examples of people not being offered a job because of findings on social networking sites.

(j) Relationships online with attending physicians, fellows, supervising residents, interns, and other medical students are all governed by the IU policy against sexual harassment. Cyberstalking, requests from those who you supervise to engage in activities outside of work, and inappropriate postings to social networking sites while supervising residents can all be considered forms of sexual harassment.

(k) Avoid giving specific medical advice.

Privacy

(a) Due to continuous changes in these sites it is advisable to closely monitor the privacy settings of your social network accounts to optimize their privacy and security.

(b) It is advisable that you set your privacy profile so that only those people whom you provide access may see your personal information and photos.

(c) Avoid sharing identification numbers on your personal profile. These would include address, telephone numbers, social security, passport numbers or driver’s license numbers, birth date, or any other data that could be used to obtain your personal records.

(d) Others may post photos of you, and may “tag” you in each of the photos. It is your responsibility to make sure that these photos are appropriate and are not embarrassing or professionally compromising. It is wise to “untag” yourself from any photos as a general rule, and to refrain from tagging others unless you have explicit permission from them to do so.

(e) Maintain the privacy of colleagues, doctors, and other IUSM or hospital employees when referring to them in a professional capacity unless they have given their permission for their names or likeness to be used.
(f) Make sure that you differentiate medical opinions from medical facts. The world of medicine is foreign to many, so readers may take your words at face value. Try to make clear what statements reflect your personal beliefs.

Confidentiality

(a) HIPAA regulations apply to comments made on social networking sites, and violators are subject to the same prosecution as with other HIPAA violations.

(b) Patient privacy measures taken in any public forum apply to social networking sites as well.

(c) Online discussions of specific patients should be avoided, even if all identifying information is excluded. It is possible that someone could recognize the patient to which you are referring based upon the context.

(d) Under no circumstances should photos of patients depicting the body parts of patients be displayed online unless specific written permission to do so has been obtained from the patient. Remember, even if you have permission, such photos may be downloadable and forwarded by others.

Patient Contact

(a) Interactions with patients within these sites are strongly discouraged. This provides an opportunity for a dual relationship, which can be damaging to the doctor-patient relationship, and can also carry legal consequences.

(b) Private patient information obtained on a social networking site should not be entered in the patient’s medical record without the patient’s knowledge and consent.

Social Media in Clinical Settings

(a) Be aware of social networking policies in each of IUSM’s affiliated hospitals.
   1) IU Health
   2) Eskenazi Health Hospital
   3) Roudebush VA

(b) Refrain from using personal social networking sites while at work or in clinical work areas.

Definitions

A resident is an IUSM resident or fellow, or a non-IUSM resident or fellow electively rotating through IUSM and provides clinical care as part of a GME program.
Social networking sites are spaces in the internet where users can create a profile and connect that profile to others (individuals or entities) to create a personal network. Examples include Facebook, LinkedIn, and Twitter.

A weblog is a website, usually in the form of an online journal, maintained by an individual with regular commentary on any number of subjects. Can incorporate text, audio, video clips, and any other types of media.

Implementation

The Designated Institutional Official (DIO) for GME is responsible for implementation of this policy.

Oversight

Policy authority for this document resides with the Graduate Medical Education Committee. The DIO and the Graduate Medical Education Committee are responsible for oversight. This policy will be reviewed every three years or more often if deemed necessary.

Forms

Social Media Policy for Eskenazi Health- attached

Related Information

The IUSM Honor Code can be found at: http://medicine.iu.edu/residents/gme-house-staff-handbook/policies-and-procedures/#Honor_Code

The IU Policy Against Sexual Harassment can be found at: http://hr.iu.edu/policies/uwide/sexual_harass.html

The HIPAA regulations in their entirety can be found at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

IU Health Social Media Site User Agreement: http://iuhealth.org/blog/social-media-user-agreement/
VA Directive 6515 (Social Media Policy)

IUSM Office of Strategic Communications:
https://medicine.iu.edu/news/communications/

History

1. Policy IUSM-GME-PO-0031 approved by GMEC and published on 12 December 2012.
2. Policy reviewed, updated, and approved by GMEC on 21 February 2018.
PURPOSE

As a teaching health care system, Eskenazi Health Health Services (“Eskenazi Health”) believes in the importance of open exchange and learning. Eskenazi Health encourages responsible communication both internally and externally in all forms and strives to maintain excellent relationships with members of the community while protecting the confidentiality of patient and institutional information. The purpose of the policy is to establish guidelines for online social media activity that protect the privacy of patients and the institution, while acknowledging an employee’s right to speak and express him/herself freely. While Eskenazi Health encourages all employees to be ambassadors for the organization in the community, it is important for employees to understand what is recommended, expected, and required when they discuss Eskenazi Health-related topics in an online forum, whether at work or on their own time. An employee’s activities in or outside of work that affect his/her Eskenazi Health job performance, the performance of others, or Eskenazi Health’s business interests are a proper focus for organizational policy.
DEFINITIONS

1. **Electronic Systems**: Any electronic system that is utilized to create, receive, access, process, store, or transmit data. This includes Eskenazi Health systems, personal, or other publicly available electronic systems. Unless otherwise specified, individuals should assume that the term Electronic Systems includes all types of accessible electronic systems. For more information and specific instructions on uses of Eskenazi Health Electronic Systems, see Hospital Administration Policy 950-79, Acceptable Uses of Electronic Devices, Media, and Systems. Information on Eskenazi Health cell phone and electronic device use can be found in Hospital Administration Policy 950-214, Use of Mobile Devices.

2. **Protected Health Information (PHI)**: Health information that identifies or, can be used to identify, an individual, and:

   a. Is created, received, or maintained by Eskenazi Health or by a business associate on behalf of Eskenazi Health;

   b. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

   c. Is stored, transmitted, and/or maintained:
      
      i. By electronic media, or
      
      ii. Any other form or medium.

3. **RelayHealth**: A secure and confidential email communication tool which is exempt from this policy.

4. **Social Media**: Web-based technology that disseminates user-generated content through highly accessible publishing techniques. This includes, but is not limited to, blogs, microblogs (e.g., Twitter), discussion forums (e.g., IndyStar.com article comments), video and photo sharing sites (e.g., Flickr, YouTube), social networking sites (e.g., Facebook), professional networking sites (e.g., LinkedIn), wikis (e.g., Wikipedia), podcasts, and other forums used for electronic social interaction.
POLICY

This policy covers all Eskenazi Health employees who use, access, or contribute to Social Media sites.

1. Patient Confidentiality and Interaction

   a. Employees shall not disclose PHI, including images and all other patient information, on Social Media sites unless expressly pre-authorized by the patient and the Public Affairs Department. Hospital Administration Policy, 950-32 Release of Information to the News Media designates those employees authorized to release information regarding patients and the organization. Unlawful disclosure of PHI on Social Media sites could violate HIPAA and other state privacy laws, resulting in sanctions, penalties and legal action. Please note that a detailed description of a patient or a patient’s condition on a Social Media site may be recognized even if all PHI identifiers have been removed. For additional information on HIPAA and PHI, see Hospital Administration Policy 950-500, General HIPAA Compliance.

   b. Employees are not authorized to use Social Media sites in a professional capacity to interact with patients, unless specifically authorized to do so by Public Affairs (e.g., HealthyMe).

   c. In instances where an employee might use Social Media to make personal contact with a patient, such activity is unacceptable if it risks confusing the patient, disrupting the therapeutic nature of the relationship, or otherwise violates Eskenazi Health policies on patient-clinician boundaries.

   d. Employees are not authorized to use Social Media sites to provide specific medical advice to patients. This can interfere with patient privacy, maintaining a consistent medical record, and other ethical considerations.

2. Compliance with Eskenazi Health Policies

   a. Employees must abide by Eskenazi Health’s Confidentiality Agreement when using Social Media. Employees shall not disclose Eskenazi Health’s confidential business or legal matters, confidential employee information, or Eskenazi Health-developed intellectual property, without authorization.

   b. Employees may not use Social Media in a way that violates Hospital Administration Policies 950-47, Anti-Harassment, 950-101, Workplace...
Employees acting in a professional capacity, or using Eskenazi Health Electronic Systems, shall not use Social Media in a manner that violates copyright or trademark rights, or infringes upon a patent, trade secret or any other proprietary rights of a party.

d. Employees acting in a professional capacity, or using Eskenazi Health Electronic Systems, shall not endorse, advocate, or lobby for legislation, political candidates, or a political party. This does not prohibit an individual’s independent participation in political activity on Social Media site during non-work time, on non-Eskenazi Health Electronic Systems, in a manner that is disassociated with Eskenazi Health.

e. Employees acting in a professional capacity, or using Eskenazi Health Electronic Systems, shall not make comments that are inconsistent with any Eskenazi Health policies or PRIDE values if the comments directly pertain to Eskenazi Health business, legal matters, employees, patients, or vendors.

f. Employees, whether acting in their personal or professional capacity, should use good judgment and be thoughtful about how they present themselves on Social Media sites. Employees are encouraged to be respectful of Eskenazi Health administration, employees, partners, competitors, and vendors.

g. Employees are not authorized to use Eskenazi Health/Eskenazi Health logos on any social media site without the approval of the Public Affairs Department.

h. When posting to personal Social Media sites and speaking about Eskenazi Health, employees should use a disclaimer that makes it clear that the employee’s views are not necessarily reflective of the views of Eskenazi Health, “The opinions expressed on this site are my own and do not necessarily represent the views of Eskenazi Health.”

i. Employees are not authorized to post pictures of Eskenazi Health employees, or other individuals affiliated with Eskenazi Health, on personal Social Media sites without the person’s prior consent, and should not post pictures of Eskenazi Health business events or
activities on personal Social Media sites without the prior authorization of the Public Affairs Department. Please refer to Section 1 with regard to patients.

3. **Professional Networking Sites**: Professional networking sites are a unique form of Social Media created specifically to enhance the development of professional contacts and professional information sharing. An individual’s affiliation or employment status with Eskenazi Health is an appropriate use of a professional networking site and does not require pre-authorization. Use of professional networking sites should comply with all other terms of this policy.

4. **Using Social Media on behalf of Eskenazi Health:**

   a. Only Eskenazi Health’s Public Affairs Department is authorized to create and/or manage Social Media sites that purport to belong to Eskenazi Health, either explicitly or otherwise. Eskenazi Health employees creating sites for Eskenazi Health business must obtain pre-authorization from the Public Affairs Department. If an employee wishes to develop a Social Media site on behalf of Eskenazi Health, he/she should develop objectives for the site, intended audience, type of Social Media forum, and how the Social Media supports Eskenazi Health’s goals while complying with the law.

   b. Eskenazi Health Social Media sites may generate media attention. Eskenazi Health’s Public Affairs Department is the organization’s designated representative to answer inquiries from the news media regarding patients or Eskenazi Health operations. Individuals should refer all media related requests for information to Public Affairs at 630-7432. Employees should not purport to be spokespersons representing Eskenazi Health without the prior approval of Eskenazi Health’s Public Affairs Department. Please see Hospital Administration Policy 950-32, Release of Information to the News Media.

5. **Monitoring and Enforcement:**

   a. Downloading or accessing inappropriate materials from Social Media sites on Eskenazi Health Electronic Systems is strictly prohibited. Eskenazi Health reserves the right to monitor equipment, electronic devices, electronic media, electronic systems, network traffic, electronic communications, and Social Media on Eskenazi Health Electronic Systems at any time for security and network purposes, and to ensure compliance with this policy. Individuals using Eskenazi Health Electronic Systems and devices consent to having their communications on these systems monitored and should not expect that their
use of Social Media through Eskenazi Health Electronic Systems is confidential.

b. In the event of Social Media misuse that violates this or any other policy, or any laws or regulations, Eskenazi Health reserves the right to ask an individual to remove user-generated content. Furthermore, any individual found to be in violation may be

subject to immediate revocation of system privileges, legal action, and/or disciplinary action, up to and including immediate termination.

REFERENCES

Hospital Administration Policy 950-32, Release of Information to the News Media

Hospital Administration Policy 950-47, Anti-Harassment

Hospital Administration Policy 950-79, Acceptable Uses of Electronic Devices, Media, and System

Hospital Administration Policy 950-101, Workplace Threats and Violence

Hospital Administration Policy 950-214, Use of Mobile Devices

Hospital Administration Policy 950-500, General HIPAA Compliance

Hospital Administration Policy 950-537, Control of Access to Information

Midtown Policy 528-24, Therapeutic Relationships and Professional Boundaries

Eskenazi Health Employee Handbook – Located on Eskenazi Health Central