I. **Policy Summary:**
The purpose of this policy is to provide UCR Health employees with requirements for participation in social media, including UC Riverside-hosted social media, and in non-UCR Health social media in which the employee’s UC Riverside affiliation is known, identified or presumed. Additionally, the policy is intended to raise awareness of internet technology misuse and potential risks including:

a. “Friending” or (being Friended) by patients on social networking sites
b. Skits showing training program rounds with inadvertent PHI and university branded materials
c. Blogs using information that can identify patients or PHI

**SCOPE/COVERAGE**
This policy applies to all UCR Health workforce members including faculty, staff and students who identify themselves with their UCR Health affiliation or use their UC Riverside email address in social media platforms such as, but not limited to, professional society blogs, LinkedIn, Facebook, Twitter, YouTube, Flickr, etc. for deliberate professional engagement or conversation. These guidelines apply to private and password protected social media as well as to open social platforms.

II. **Definitions: N/A**

III. **Policy Text:**
A. Workforce members are expected to adhere to UCR Health compliance requirements and the University of California Ethical Guidelines, the UCR School of Medicine Code of Conduct, Conflict of Interest policies and University HIPAA policies, when using or participating in social media. All rules that apply to other UC Riverside communications apply here, specifically: respecting patients, customers, and one another; protecting confidentiality, privacy and security; and safeguarding and proper use of UC Riverside assets.

B. **No Protected Health Information** or information that could be used to identify a patient should ever be posted to an internet site, or discussed in a social networking site.

C. Only University employees authorized by their Departments may use social networking
web sites to conduct university business. The use must also be reviewed and approved for site content and appropriateness of material by the UCR School of Medicine Communications Office. Workforce members may not provide a link from their site to a UC Riverside site without the express written permission of the UCR School of Medicine Communications Office.

D. Personal use of University electronic resources to access social networking sites is limited to incidental use and should be done during personal (non-work) time only. Incidental use must not interfere with an individual’s performance of his/her assigned job responsibilities or someone else’s job performance, or compromise the functionality of the department or campus network. However, due to the security risk posed by malicious software, internet access using UCR Health computers may be limited based on the location of the computer. Please refer to UC Riverside policy on “Computer Systems Access, Use, and Security, Campus Policy Number: 400-35.

E. Individuals or groups within the University community are not permitted to present personal opinions in ways that imply endorsement by the University. If posted material may reasonably be construed as implying the support, endorsement or opposition of the University with regard to any personal statements, including opinions or views on any issue, the material shall be accompanied by a disclaimer: an explicit statement that the individual is speaking for himself or herself and not as a representative of the University or any of its offices or units. Refer to University policy regarding the use of the University’s name.

F. Workforce members may not post material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to any person or entity when posting to UC Riverside hosted sites.

G. Workforce members may not post content or conduct any activity that fails to conform to any and all applicable state and federal laws. It is critical that workforce members abide by the copyright laws by ensuring that they have permission to use or reproduce any copyrighted text, photos, graphics video or other materials owned by others.

IV. Responsibilities: N/A

V. Procedures:

A. All official medical activities, images, records and notes, must be kept in official University applications and tools such as secure sharepoints, share drives, and not on social network sites.

H. Riverside computer resources may be limited in some areas due to the increased security risk of contamination with malicious software. Please refer to UC Riverside policy on “Computer Systems Access, Use, and Security, Campus Policy Number: 400-35.

B. Professional relationships with patients should not be conducted on social networking or internet sites.

C. Take extreme care with privacy settings when setting up personal profiles on these sites. Control who can look at your profile, personal information, and photos. You may be able to limit access somewhat but not completely. You have no control over what someone else may share.

D. Exercise appropriate discretion when using social network sites for personal communication (with friends, colleagues, etc.) with the knowledge that your behavior may be observed by patients, colleagues, and others.

E. Never provide medical advice via a social networking site.

F. Never post protected health information on a social network site.
G. If you publish a blog or post to a blog and it has something to do with the work that you do, you must make it clear that the views expressed in the blog are solely your personal views and do not necessarily represent the reviews of UCR Health.

H. Remember that any information you post to the internet is public information and could be googled or searched by family, friends, patients, colleagues or supervisors.

I. Content contributed on all platforms becomes immediately available on the internet, and leaves the contributing individual’s control.

J. No identifiable photos of patients or staff members should ever be posted without their written authorization.

K. If someone from the media or press contacts faculty, staff or students about postings on forums that relate to UCR Health in any way, faculty/staff/students must alert their managers and notify UCR SOM Communications Office before responding.

L. If someone offers to pay faculty, staff or students for participating in a forum due to their UCR Health role, offers advertising for pay and/or for endorsement, University policies apply regarding vendor relations, conflict of interest and compensation plan requirements.

M. In response to concerns, complaints or information provided by individuals regarding potential privacy breaches, University administrations may look up profiles on social networking sites and may use the information in informal or formal investigations and proceedings.

N. Staff should consult their supervisor, manager, the UCR SOM Communications Office or the Compliance and Privacy office if they have any questions regarding this policy.

VI. Forms/Instructions:

Attachment A: UCR School of Medicine: Best Practice Guidelines for Social Media

VII. Contacts:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Title</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Compliance and Privacy Officer</td>
<td>(951) 827-4672</td>
</tr>
<tr>
<td>Compliance</td>
<td>Privacy Analyst</td>
<td>(951) 827-7672</td>
</tr>
<tr>
<td>Communications</td>
<td>Director of Communications</td>
<td>(951) 827-4598</td>
</tr>
</tbody>
</table>

VIII. Related Information: N/A

IX. Revision History: N/A

Approval(s)

James R. Herron
Compliance and Privacy Officer
School of Medicine
Attachment A

UCR School of Medicine: Best Practice Guidelines for Social Media
(Revised July 11, 2013)

The UCR School of Medicine encourages the use of social media to connect to the broader campus community and the general public around the world. The long-term success of any social media community depends on a mutually shared philosophy of respectful behavior. Toward this end we offer the following best practice guidelines in keeping with the standards of the UCR School of Medicine and the medical profession at large.¹ ³

Be respectful: Refrain from posting material that is profane, hateful, threatening, abusive, harassing, obscene, pornography, nudity, libelous, defamatory or embarrassing to another person or entity. Be respectful of the rights and opinions of others.

Be honest and transparent about who you are: While you may certainly acknowledge that you are a student of the UCR School of Medicine, unless you have been authorized by University Public Relations, you should not portray yourself as a spokesperson or even an unofficial spokesperson. Avoid the use of official School or University logos, insignias, banners, badges, emblems, brands, etc. that may mistakenly give this impression to others or the public. If you are using social media for your profession identity and use, consider a separate venue for your personal and private life.

Respect confidentiality: Refrain from discussing private conversations other than with those directly involved. Never discuss patient care details or post pictures or images that may identify individuals.

Live by the law: Do not post content that violates any state or federal laws, most notably those applicable to patient confidentiality and privacy (i.e. HIPPA). Always obtain written permission to use or reproduce copyrighted material or proprietary information.

The Internet is a public space: Remember that social media sites are public, no matter what privacy settings may be in place. Consider, in most cases, everything you post online will be seen by a public audience. Assume everyone is reading your post, no matter how obscure or secure the site to which you are posting may seem.

Use the “pause-before-posting” approach¹: Reflect on how the general public may perceive the content about to be posted. While you speak for yourself, the public will often perceive your actions reflecting UCR and the medical profession at large. Have you listened carefully? Is your post adding value to the discussion? Is the post helpful? Have you been courteous, sensitive and respectful?

¹These guidelines apply to personal use of social media. Social Media is defined as any electronic communication through which users create online communities to share information, ideas, personal messages, and other content. These include social networking sites (e.g. Facebook, Twitter), media-sharing sites (e.g. Flickr, YouTube) blogs, wikis, and podcasts among others. Use of official School of Medicine or UC Riverside social media sites are governed by existing policies by UCR public relations and university Administration. These guidelines are not intended to supersede existing related policies within the University or School of Medicine (e.g. Student Handbook, UCR SOM Code of Conduct) or pertinent local, state or federal regulations (e.g. the Health Insurance Portability & Accountability Act - HIPAA).
Safety Tips for Online Social Media & Networking: Self-Reflective Questions
(Revised July 11, 2013)

1) Did I set my privacy setting to help control who can look at my profile, information, and photos? While you can limit access somewhat, it is by no means complete. You have no control over what someone else may share about you.

2) How much information about yourself do you want people to know about you? With whom will your “friends” share this information? Not everyone will respect your personal or physical space.

3) Would I post this material on a roadside billboard or a television commercial? What would a stranger think about my post? What about my parents?

4) What image am I projecting about me? my School? my University? and the medical profession at large? Remember that what you post leaves a “digital footprint” that is both public and can last in perpetuity.¹ What might a patient think about my post? What would a future employer or residency program director think after seeing this post?

5) Have I asked permission to post someone else’s image or information? Am I infringing on someone else’s privacy? Could I be hurting someone? Could I be the subject of a judiciary hearing? Could I be the subject of a libel or legal suit?

6) Does my equipment have the proper spyware and virus protection installed? Many social networking sites collect profile information to SPAM you. Others contain links that can infect your equipment with viruses that potentially can destroy data and infect others with whom you communicate.

Cited References:
