TITLE: PERSONAL AND PROFESSIONAL USE OF SOCIAL MEDIA

PURPOSE: To provide authorized users of University Health System (Health System) information assets with requirements for participation in social media, including Health System-hosted social media, and non-Health System social media, through which the user's Health System affiliation is known, identified, or presumed. [Key words: Protected Health Information (PHI), privacy, social media, disclosure, integrity.]

POLICY STATEMENT:

The Health System acknowledges and respects the right of employees to use social media on their personal time and using personal electronic devices. Social media access through Health System-owned equipment, however, is for business purposes only and is restricted. This policy establishes boundaries for employees as they create and use personal social networking technologies.

POLICY SCOPE:

The lack of explicit reference to specific social media and attendant communications does not limit the scope of this policy. Where no explicit policy statement exists, employees should use their professional judgment and take the most prudent action possible regarding use of social media. Employees are encouraged to consult with the Corporate Communications and Marketing Department if they have any questions.

In publishing this policy, the Health System is not assuming duty to monitor social media or other public communications, but reserves the right to take appropriate action in accordance with this policy at its sole and absolute discretion.

Social media access through Health System-owned equipment is restricted to the Corporate Communications & Marketing and Information Assets departments, and other users authorized to post or manage specific social media assets on behalf of the Health System.

POLICY ELABORATION:

I. DEFINITIONS

A. Authorized Users – Authorized users of University Health System information assets include all employees, house-staff, affiliated providers, volunteers, contractors and other persons provided with a Health System network user name and password or authorized to manage social media assets on behalf of the Health System.

B. Blog - A website that allows an individual or group of individuals to share personal commentary, observations and opinions with online audiences.

C. Podcast – A collection of digital media files distributed over the Internet, often using syndication feeds, for playback on portable media players and personal computers.

D. Protected Health Information (PHI) – Any information, whether oral, written, electronic or recorded, in any form or medium (including demographic information collected from an individual) that identifies or may be used to identify the individual and that relates to:

1. The past, present or future physical or mental condition of an individual;
2. The provision of healthcare to an individual; or
3. The past, present or future payment for the provision of healthcare to an individual.

E. Social Media – Any tool or service that uses the Internet to facilitate conversations or provide a forum for discussion. Social media includes items such as blogs, photo and video galleries, podcasts, discussion forums and social networks. Current examples include, but are not limited to, Facebook, Twitter, LinkedIn, Instagram, Snapchat, YouTube, and Flickr.

II. INFORMATION AND REQUIREMENTS REGARDING SOCIAL MEDIA USE:

A. Official University Health System Social Media Initiatives

1. The Corporate Communications & Marketing Department is responsible for managing all Health System social media assets, and, as deemed appropriate, may designate or authorize Health System areas to access social media for administrative or investigative purposes, and to post content or serve as administrators for specific social media profiles.

2. Personal Health Information, including patient photographs, will

only be shared with permission obtained through the Health System's Consent for Photography/Video/Audio form. (Policy No. 2.03, Release of General and Patient Information and Policy No. 2.1401, Uses and Disclosures of Patient Health Information)

3. The Health System does not endorse people, products, services and organizations. Official Health System social media assets should not be used to provide such endorsements.

4. Any employee wishing to develop a social media initiative or project must submit a proposal to Corporate Communications & Marketing for approval prior to anything being posted online about the Health System.

B. Personal use of social media by University Health System staff and physicians

1. Employees are permitted to use their personal devices for social media during breaks, in non-patient care areas. Employees may not use social media during work hours or use Health System equipment to access social media (Policy No. 2.08.02).

2. Employees may not use their Health System email addresses (@uhs-sa.com) for personal blogs and social networking on personal or other non-Health System hosted sites.

3. Personal blogs and social media pages containing content on about the Health System must be written in the first person and clearly indicate that the employee is speaking for him/herself and not on behalf of the Health System. Health System logos and trademarks may not be used on employees' personal social media.

4. Patient PHI including patient images must never be posted directly by employees or physicians on personal social media or websites. Employees and physicians may "like" or "share" any posts on the Health System's official social media pages, as the administrators of these pages always obtain appropriate consent prior to posting any PHI.

5. Disclosure of Health System confidential or proprietary information is explicitly prohibited.

6. Employees' online postings that in any way reference or contain content about the Health System must be consistent with the Health System's mission, vision, values and brand. This includes

photographs of employees or physicians in Health System branded clothing, content, as well as "likes," "shares" or other social reactions of employees or physicians who publicly identify themselves on these online platforms as working at any University Health System location. Employees are prohibited from posting anything obscene, vulgar, defamatory, threatening, discriminatory, harassing, abusive, hateful or embarrassing to or about employees, patients, locations or visitors.

7. Employees should be aware that, regardless of their privacy settings, personal online comments and images can be captured and forwarded by others and are subject to this policy.

8. Employees in patient care roles and physicians should not initiate or accept friend requests except in circumstances where a personal relationship pre-dates the treatment relationship.

9. Staff in management/supervisory roles should not initiate social media connection requests with employees they manage. Managers/supervisors may accept friend requests if initiated by the employee.

III. POLICY VIOLATIONS:

A. Users encountering suspected violations of this policy should immediately report the incident to their supervisors or the Human Resources department. Upon receiving a report of violation, the supervisor is responsible for ensuring notifications are made to relevant departments:

1. Information Services should be notified immediately in cases where technology assets may be involved.
2. The Integrity Services department should be immediately notified when patient privacy may have been breached or other Health System policies violated.

B. Each incident will be reviewed on an individual basis and, where appropriate, the supervisor and Human Resources will determine disciplinary action, up to and including termination of the employee. In addition, Information Services may revoke access to computer systems assets if the violation is determined to put such resources at risk. The Integrity Services department

will investigate and respond to all reported breaches of patient privacy in accordance with Corporate Policy No. 2.14.01, Uses and Disclosures of Protected Health Information

C. Violations of local state and federal laws may subject persons to penalties including fines or imprisonment or both. The Health System reserves the right to pursue legal action as appropriate.

D. Licensed healthcare professionals should consult with respective licensing agencies for more information regarding impacts on licensure for violation of patient privacy regulations.

REFERENCES:

Corporate Policy No. 2.03, Release of General and Patient Information
Corporate Policy No. 2.08.02, Information Asset Security/Use
Corporate Policy No. 2.1, Integrity Program
Corporate Policy No. 2.14.01, Uses and Disclosures of Protected Health Information
University Health System Employee Handbook
American Medical Association Report on Professionalism in the Use of Social Media
National Council of State Boards of Nursing
https://www.ncsbn.org/NCSBN_SocialMedia.pdf

OFFICE OF PRIMARY RESPONSIBILITY:

Sr. Vice President, Strategic Communications & Patient Relations