Social Media Liability: Effective Strategies to Minimize Risk

Most healthcare organizations have established a social networking presence in order to educate the public, connect with potential patients and enhance communication with staff and providers. Social networking generally includes all types of online postings and/or interaction. Typically, organizations create networking channels by linking their own website to the following types of media platforms:

- *Social networking sites* to promote sharing of news and information (e.g., Facebook).
- *Video and photo sharing sites* to facilitate rapid exchange of documents and images (e.g., Instagram, YouTube, Google Docs).
- *Micro-blogging sites* to encourage interaction via short published messages and links (e.g., Twitter).
- *Weblogs* to communicate ideas and opinions in journal or diary format (e.g., corporate, publication and personal blogs).
- *Business networks* to connect job seekers and potential partners to the organization, and colleagues with each other (e.g., LinkedIn, XING).
- *Forums and discussion boards* to support sustained dialogue among community members (e.g., Yahoo! Groups, Google Groups).

These and other emerging platforms encourage dialogue between providers, colleagues and patients, enriching professional collaborations and leading to stronger, more successful patient relationships. Their misuse, however, can invite exposure to such perils as unauthorized disclosure of protected patient information, bodily injury due to inappropriate content, infringement of copyright or trademark, and network infiltration. This edition of *AlertBulletin®* offers practical strategies to help organizations obtain the advantages of social media while mitigating associated risks.

PREPARATORY MEASURES

A healthcare organization's use of social media should support its mission of patient advocacy, as well as positions on public policy matters. Before initiating a new networking activity, a Social Media Steering Committee – comprising professionals from risk management, legal, marketing, information technology and security, and healthcare information records management – should determine basic parameters. The following questions can help focus the planning process:

- *Which media platform, tool or application is best suited* for the desired purpose?
- *Who is the intended audience* for the site?
- *What topics, activities and forms of interaction will be promoted,* and what will be discouraged?
- *What resources are available* for the project?

Some organizations retain an interactive marketing/social media manager to assist with the following planning functions:

- *Conducting preliminary vendor assessments* of selected media sites and communities for reported security weaknesses, utilizing the National Vulnerability Database, among other resources.
- *Reviewing insurance policies for potential coverage gaps* and recommending portfolio changes, where necessary.
- *Establishing practical boundaries and guidelines* for electronic media use. See CNA *AlertBulletin®* "Electronic Media: Sound Policies Maximize Benefits, Minimize Improper Use." Updated 2017.
- *Promulgating sound operating rules and security controls* to protect against infiltration and other external threats.
- *Negotiating with vendor platforms regarding terms of use*, such as requirements for separate login pages and written notice of changes in privacy conditions and provisions.

Once the site becomes active, the social media manager can also help educate users on rules and etiquette, monitor online discussions, enforce guidelines, review and update vendor contracts and site controls, and ensure that all social media tools have a consistent look and feel, including use of the institution's logo.

SOCIAL MEDIA SAFEGUARDS

The following measures are designed to help improve compliance with social media use expectations and limit liability exposure:

Written policies and procedures. The Social Media Steering Committee should issue written guidelines that protect data integrity, prohibit misleading and harassing statements, and designate individuals who can speak on behalf of the organization. Guidelines should also ensure that legal counsel and information technology staff review vendor operating policies, along with contract provisions for privacy obligations and security controls.

Guard against breaches of patient privacy. The following core responsibilities help social media users safeguard patients' protected health information (PHI) or other sensitive data:

- *Store all PHI or other sensitive data in secure server environments only*, such as in a directory or network file server.
- *Require documented approval before copying or downloading PHI or other sensitive data to a storage device*, such as a local hard drive, flash drive, CD or laptop.
- *Prohibit staff from using personally owned portable devices (e.g., cellular phones, smartphones, tablets and laptops) for work-related purposes*, unless specifically approved by management.
- *Protect PHI or other sensitive data from unauthorized access through the use of effective security measures*, including, but not limited to, password protection techniques, encryption software, anti-malware software, and hardware and software firewall protection.
- *Utilize encryption technology when accessing wireless networks*, such as a two-factor authentication process, in order to secure information transfers.
- *Back-up authorized portable devices in accordance with the information technology department's guidelines*, making sure not to utilize personal home computers or public workstations and servers.
- *Maintain a log of authorized data destruction*, listing the device, date of destruction, description of the PHI or other sensitive data disposed of, and the name of the individual who is responsible for destroying the data.
- *Instruct staff not to share authorized portable devices with family members and friends*, and require them to promptly report to a supervisor the loss or theft of any authorized device, hardware or electronic media.

Staff training. Training should be offered to all new employees and annually thereafter. Sessions should cover such key concerns as social networking rules and etiquette, parameters for use during working and non-working hours, potential legal perils, patient confidentiality issues and disciplinary consequences for misuse. Training session content and attendance should be documented.

Standard terms of use. Users should be informed that they are subject to the site's terms and conditions and that any violations will result in termination of access. The "click agreement" with users should be written in clear and unambiguous language and include these essential provisions, among others:

- *Users understand the risks associated with interactive media*, and acknowledge that postings by providers and staff are not intended to be medical diagnosis or treatment.
- *Service marks and trademarks of the organization are the sole property of the organization*, and no copyrighted text, image, video or audio content may be distributed, modified, reproduced or used, in whole or in part, without prior consent of the organization.
- *Blog postings may be edited or deleted without prior notice*, and abusive, illegal, disruptive or medically misleading communications are subject to immediate removal.
- *Use and disclosure of patient health information shall be carried out pursuant to patient privacy policies* and relevant federal and state privacy laws, and any solicitation of confidential or proprietary patient information is prohibited.
- *The organization is indemnified against any damages, liabilities, judgments or expenses* arising from any third-party claim involving posted material.

Disclaimer statements. The following statements are standard:

- *All content and information are of an unofficial nature* and are not intended to be interpreted as medical advice.
- *The views expressed are those of users* and are not necessarily representative of the organization.
- *The organization is not obligated to monitor chat rooms*, bulletin boards or other interactive areas where visitors post their comments.

Editorial controls. Written guidelines for user-posted comments should include the following restrictions:

- *No material will infringe on the rights of any third party*, including rights to intellectual property, privacy or branding.
- *Any off-topic material may be deleted*, including the promotion of outside products, services, groups or organizations.
- *No unlawful material can be posted on the site*, nor any content that could be considered obscene, defamatory, threatening, harassing or hateful.
- *The organization reserves the right to remove posts advertising commercial products*, including business solicitations, chain letters or pyramid schemes. Platform settings should disable advertisements when possible.
- *Postings cannot contain specific patient data* or other confidential information.

Incident response plan. A written plan should address violations of site rules, such as password compromise or sharing, data/site disfigurement or posting of unauthorized patient images. The plan should minimally encompass crisis response, documentation and reporting protocols, follow-up action and disciplinary standards (in compliance with relevant employment laws).

Would you like to read *AlertBulletin*® online? Visit **www.cna.com/ healthcare**, click on "Search CNA" in the top right-hand corner of the screen, type the article's full title in the search box and then click on the magnifying glass icon.

MEDIA LIABILITY COVERAGE

A directors and officers policy may not provide sufficient coverage for risks associated with social networking sites. For this reason, healthcare organizations with extensive online presence should consider securing specialized coverage for certain losses relating to social media sites, provider blogs and web-based publications.

Consult your insurance agent, broker and/or underwriting representative regarding potential coverage gaps and available data privacy and media liability policies. Innovative products – such as media contingent bodily injury liability coverage – are designed to complement an enterprise-wide risk management program. To learn more, contact your local CNA underwriter.

QUICK LINKS

- Backman, C. et al. "Social Media + Healthcare." *Journal of AHIMA*, March 2011, Volume 82:3, pages 20-25.
- Neighbor, J. "10 Things Every Health Care Professional Should Know About Social Media," Columbia University Medical Center, *Community News*, posted August 15, 2013.
- U.S. Department of Health & Human Services, Policies that Apply to Social Media.
- U.S. Department of Health & Human Services, Social Media Resources.
- Ventola, C. L. "Social Media and Health Care Professionals: Benefits, Risks, and Best Practices," *Pharmacy and Therapeutics*, July 2014, Volume 39:7, pages 491-499.

CNA

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare.