ALERTBULLETIN®

CNA
We can show you more.®

AB REPUBLISHED 2017

Electronic Media: Sound Policies Maximize Benefits, Minimize Improper Use

The following cases demonstrate the potential impact of careless electronic communication on malpractice litigation:

- An aging services caregiver took photos of a resident during a daily shower. He posted the photos on his personal Facebook page and Instagram account. Colleagues later discovered the photos and reported the incident to the aging services organization's administrator. The caregiver was terminated from the staff. The organization subsequently reported the caregiver's actions to the state licensing board for investigation and disciplinary action.
- An operating room nurse was texting personal messages during a long surgery. The patient sustained complications during the procedure and sued the hospital for damages. During discovery, the plaintiff's attorney secured records of the nurse's text messages and used them as evidence of inattentiveness and substandard practice.
- A pediatrician was sued by the parents of a child who died from complications of diabetes. Under a pseudonym, he blogged about his courtroom experiences, discussing such sensitive topics as jury preparation tactics and defense strategy. Late in the trial, the plaintiff's attorney accessed the blog and identified the defendant as its writer. The next day, the physician settled the case for a substantial amount.

Electronic media – including text and e-mail messaging, blogs, social networking sites and posted videos – have become a primary means of self-expression. The ever-growing volume of online communication and instant messaging has created a new sense of connectedness – as well as a new cluster of risks, including electronic discovery requests that may encompass text messages, blog entries and social media postings.

Administrators and risk managers in all healthcare settings must understand the exposures associated with these media and create policies that recognize their benefits while minimizing the potential for misuse. This *AlertBulletin*® examines risk exposures associated with electronic media use and offers general policy recommendations for the workplace environment. For a discussion of the exposures and policy considerations specific to social media use, see CNA *AlertBulletin*® "Social Media Liability: Effective Strategies to Minimize Risk." Updated 2017.

ISSUES OF CONCERN

Uncontrolled use of social media and electronic devices by staff members may result in the following exposures, among others:

Organizational liability and impact on litigation. Harassing, threatening or otherwise inappropriate messages and videos posted by employees from workplace computers, laptops and tablets, or texted from employer-issued mobile telephones, can create vicarious liability exposure for an organization. And as seen above, improper litigation-related postings and text messages can undermine legal defense efforts.

Patient/resident privacy. Workplace e-mail or text messaging may violate privacy and security requirements imposed under HIPAA and the regulations promulgated under the law. If protected health information (PHI) is revealed on organization-owned equipment or employee-owned devices used for healthcare-related purposes, this could constitute a breach of the HIPAA Privacy and Security Rules, as well as related state laws. Also, the use of cellular telephones and smartphones to take and share photographs relating to a patient/resident has significant privacy implications.

QUICK LINKS

- Barrett, C. "Healthcare Providers May Violate HIPAA by Using Mobile Devices to Communicate with Patients." *ABA Health eSource*, October 2011, Volume 8:2.
- Mobile Electronic Device Use in the Emergency Room, Emergency Nurses Association, September 2013.
- Seaman, B. "7 Best Practices for HIPAA Mobile Device Security." *Health IT and CIO Review*, posted November 22, 2013.
- Spector, B., et al. "Guidelines for Using Electronic and Social Media: The Regulatory Perspective." *The Online Journal of Issues in Nursing*, September 2012, Volume17:3, Manuscript 1.

Workplace productivity and patient/resident safety. Texting and conversing on mobile telephones and tablets in care areas may decrease staff efficiency and lead to distraction and error, endangering patients/residents. Even the use of headphone devices can create a sense of disconnection from the environment, impairing communication and slowing response time.

Network security. Unregulated Web browsing and messaging on networked computers and portable devices, such as cellular telephones, smartphones, iPhones, Android devices, iPads, laptops and portable workstations, can introduce viruses or spyware into the system, resulting in possible data loss, theft or damage. In addition, sharing of passwords or other security lapses can compromise confidential information, with potentially serious regulatory and liability implications.

Risk to reputation. Utilizing social media forums to recruit new patients/residents or build loyalty may end up harming an organization's reputation, unless the effort is managed in accordance with best practice guidelines. Exposures include, but are not limited to, jurisdictional issues and allegations of fraud and defamation.

Human resources policy should directly address the issues raised by the proliferation of electronic media, in order to clarify organizational expectations and reduce liability exposure.

POLICY RECOMMENDATIONS

Human resources policy should directly address the issues raised by the proliferation of electronic media, in order to clarify organizational expectations and reduce liability exposure. The strategies that follow are intended to help administrators draft general guidelines for the use of these communication tools:

Create and enforce a formal policy governing personal use of networked computers and portable devices, with provisions that strictly ban all messages and activities of an offensive, threatening, harassing, defamatory or unprofessional nature. Request that employees sign an acknowledgment form confirming that they understand the rule and the consequences of noncompliance. Signed forms should be retained in human resources files.

Notify staff in writing of monitoring policies. Explain that employers have the right to monitor e-mail and text messages along with other electronic communications on facility-owned devices and that inappropriate conduct may have disciplinary consequences, up to and including termination.

Regulate mobile telephone use by staff members, specifically addressing such key issues as personal calls while on duty, confidentiality, conversational volume and etiquette, talking while driving and utilization of the camera feature. Issue separate and stricter policies for work-issued mobile telephones, reflecting the organization's vulnerability to vicarious liability.

Revisit the organization's privacy and confidentiality policies, taking into consideration the risks of posted and texted messages and videos containing PHI or other sensitive material. Revise outdated policy statements to ensure compliance with the HIPAA Privacy and Security Rules.

Convey to staff the possible implications of careless use of social media, including the permanence and recoverability of even deleted messages, limits of anonymity and realities of e-discovery. Clearly describe both the nature of the risks and the consequences of policy violations in the employee handbook, and use staff training sessions to reinforce the importance of sound judgment.

Draft specific guidelines addressing the need for discretion during litigation and discovery. Also, remind physicians and staff members that, as a threshold requirement, they must receive written authorization from patients/residents prior to discussing their cases on blogs or websites. Postings should not include individually identifiable information.

Ensure that both legal counsel and information technology staff review all social media-related policies for regulatory compliance and technical relevance.

Encourage appropriate etiquette and a mature attitude. Remind staff members that they are viewed as ambassadors of the organization, and their posture online should reflect this fact. Consider assigning mentors to coach less experienced staff in understanding the nuances of professional conduct.

Regularly underscore cyber security rules and concerns, using orientation and training sessions, web-based tutorials, posters, supervisory reminders and other means.

Foster constructive use of social media. Many organizations creatively utilize this technology for purposes of outreach, reputation management and emergency communication. Written policy should address the following important considerations:

- Guidelines for engaging e-patients.
- Protocols for managing online conversations.
- Parameters for giving patients both personal medical advice and general medical information.
- Procedures for combining social media with healthcare information records.
- Criteria for disengaging e-patients (e.g., publishing derogatory statements or falsehoods about the organization).

Electronic media define connection in today's world. Healthcare administrators should establish a balance between staff members' reliance on these ubiquitous communication tools and the perils posed by their misuse. The measures described in this resource can help organizations minimize risk by providing employees the guidance they need.

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.

CNA

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