

## Communicating through Social Media

### OVERVIEW OF ISSUE

Social media refers to various electronic communication channels that enable the creation, sharing, and interactive participation of messages, content, and information with friends, family, colleagues and the public. Social media also provides a forum for healthcare providers to share updates about the organization, including services, alerts, events, and news, fundraising events and patient educational events. Key mitigation strategies to reduce misuse of social media include having a policy and an education plan that addresses privacy, reputation and human resources risks.

### KEY POINTS

- Ensure adequate security and privacy controls are in place for applications which allow healthcare providers to communicate directly with patients.
- Once something is online, assume it will never be completely deleted.

### THINGS TO CONSIDER

#### Concerns related to Social Media

Organizational and professional concerns related to misuse of social media include ethics, professionalism, privacy and confidentiality, cyber bullying and information quality. Usage of social media and related policies must be in compliance with the organization's devices security, privacy and code of conduct policy. Keep in mind that all content may be discoverable (and subject to Freedom of Information requests).

#### Policy & Procedures

Consider implementing a social media plan/policy and ensure that a staff education plan is developed and implemented. The plan/policy should include but not limited to:

- Management:
  - Identify who has the authority to set up a social media account that represents the organization.
  - Identify who will officially speak on behalf of the organization.
  - Code of Conduct or Respectful Workplace (i.e. disparaging comments) expectations.
  - Process to respond to breaches in patient and staff privacy.
  - Process for managing risks related to reputation management, inappropriate or unprofessional use or postings.
  - Use of social media related to candidate screening.

- Content Development and Monitoring:
  - Identify who will be responsible for content development.
  - Provide direction on posting i.e. photos, videos, names or identifiable information of patients and staff (obtain consent).
  - Identify who will be responsible for monitoring and responding to activities or negative comments made about the organization according to a response/escalation process.
- Staff using Social Media:
  - Direction for staff regarding account security related to using professional devices or personal devices for work (e.g. bring your own device arrangements).

#### Staff and Physicians:

If using the healthcare organization's social media platform, professional, student or personal platform remember to:

- Maintain professionalism at all times and accurately state credentials.
- Maintain appropriate boundaries of the patient-caregiver relationship in accordance with Regulatory College and organizational guidelines and do not

## Communicating through Social Media

extend or accept 'friend' requests to/from patients, substitute decision-makers, patient's family or management to whom you report.

- Protect patients, staff's personal confidentiality and privacy.
- Be honest in all professional interactions.
- Do not speak on behalf of the organization unless authorized to do so and identify whether the submission is representative of the organization or a personal comment.
- Maintain separate personal and professional channels/accounts on social media platforms.
- Be aware of social engineering scams. Do not respond to requests for confidential information (e.g. banking information) received through social media.

### Using Social Media for Patient Care

- Security and Privacy settings
  - All practices should be in compliance with organizational policy and procedures

- Use secure closed systems with the highest privacy and security settings. (E.g. ensure no one other than the account administrator can post on your organization's Facebook timeline/wall. Turn on approval features so that individuals have to request to be your follower.)
- Consult your technical expert to ensure the highest level of security and privacy settings have been chosen for the accounts.
- Communicating with patients
  - Advise patients of organization approved and secure methods
  - Patients should be made aware of the benefits and limitations of the communications tool including the privacy protections and must provide consent to participate given these provisions.
  - Establish expectations of message response time, how emergencies should be handled, and issues that should be handled online vs. in-person.



## REFERENCES

- HIROC. (2015). Privacy breach. [Risk Reference Sheet].
- American Hospital Association. (2015). [A hospital leadership guide to digital and social media engagement](#).
- American Medical Association. (2011). Opinion 2.3.2 – [Professionalism in the use of social media](#).
- Cain, J. (2011). Social media in health care: The case for organizational policy and employee education. *Am J Health Syst Pharm*. 68(11),1036-1040.
- Cavoukian A. (n.d.). [When online gets out of line: Privacy – Make an informed online choice](#). *Information & Privacy Commissioner of Ontario and Facebook*.
- Chretien K C, Kind T. (2013). [Social media and clinical care: Ethical, professional, and social implications](#). *Circulation*, 127(13),1413-1421.
- CNA Financial (2015). Webinar: Privacy and security breaches in the health care environment: Understanding preventing [PowerPoint slides].
- Grajales F J, Sheps S, Ho K, et al. (2014). [Social media: A review and tutorial of applications in medicine and health care](#). *J Med Internet Res*. 16(2), e13.