AMERICAN SOCIETY OF PLASTIC SURGEONS®
444 East Algonquin Road
Arlington Heights, IL 60005-4664
847-228-9900
Fax: 847-228-9131
www.plasticsurgery.org

AMERICAN SOCIETY OF PLASTIC SURGEONS

ASPS Guiding Principles: Online Communication for Plastic Surgeons

The American Society of Plastic Surgeons recognizes that the increasing use of the Internet to enhance practice visibility and educate consumers has become a widespread practice. In fact, the use of a well designed informative website is considered by many to be an essential element of their marketing plan. Maximizing the use of online technology by offering physician-patient email, online chat opportunities, online social networking exchanges, online consultations, pre-screening services, and post-operative check-up services is an attractive option. However, these practices may increase a physician's liability risk. Thus, before initiating an online patient relationship, physicians should be aware of the medico-legal aspects associated with online communications.

1. Background

- **Online Communication and the Physician-Patient Relationship**
  A physician-patient relationship typically begins when a physician provides a patient with individualized professional advice or treatment during an in-person visit or an electronic exchange via email, telecommunication equipment, instant messaging service, or phone regardless of reimbursement. However, health or procedural information accessed by a patient from a physician's website for general information purposes only, without personal interaction, should not constitute a physician-patient relationship.

- **Electronic Transmission of Protected Health Information**
  Compliance with the Health Insurance Portability and Accountability Act of 1996 requires vigilance on the part of the physician to ensure that confidential and private information is securely transmitted. The Department of Health and Human Services recommends that HIPAA covered entities utilize email encryption programs when transmitting protected health information (PHI) to patients through email. Encryption programs transform information transmitted through the email exchange into an unreadable mathematical algorithm. In order to access this information, users must type in a decryption key to unscramble the data.[1]

- **Social Networking Issues**
  Social networking sites such as Facebook, Twitter, and Realself offer plastic surgeons the unique opportunity to connect with prospective and established patients. It is a common trend for patients to post comments or questions about plastic surgery procedures to a physician's personal social networking page. Physicians should be aware that responding to patients' posts with a specific treatment regimen may establish a physician patient relationship and may violate HIPAA, in either case significantly increasing a physician's risk for liability.

- **Regulatory Environment: Providing Inter-State Consultations**
  Currently, thirty-two states (and the District of Columbia) require full medical licensure by that state to provide online telemedicine services, including diagnosis, consultation, treatment, transfer of medical data, and education, to in-state patients. Sixteen states offer a "special purpose" license for physicians practicing across state lines.[2]

2. Guiding Principles

1. Prior to the initiation of online communication between physician and patient, physicians should:
   a. understand that a physician-patient relationship typically begins when he/she provides the patient with professional advice or treatment;
   b. understand that the standard of care for online medical relationships between surgeons and new or established patients, regardless of which type of online technology is utilized, remains the same as traditional office visits;
   c. ensure that informed consent is obtained from the patient regarding the appropriate use and limitations of this form of communication;
   d. ensure patients are clearly informed about any charges that might be incurred, and be made aware that they will be responsible for charges not covered by the patient's health insurance;
   e. understand that it is the individual physician's responsibility to abide by all applicable local and state regulations, including (in some cases) the laws and regulations of the location of the patient in addition to the physician's location;
   f. understand that online interactions between a healthcare clinician and a patient may be subject to requirements of state licensure and online communications with a patient, outside of the state in which the physician holds a license, which may subject the clinician to increased risk. [2,3]

2. Physicians should exercise discretion when selecting patients for the use of online services. Online communications of any kind are best suited for established patients who have been previously seen and evaluated in an office setting.[3]

3. When communicating with an existing patient, the physician:
   a. is responsible for distinguishing between an online consultation related to a known pre-existing condition and the diagnosis and treatment of new conditions addressed for the first time online. The diagnosis and treatment of new conditions online may compromise patient safety and increase liability exposure;
   b. should ensure that a permanent record of online communications relevant to the ongoing medical care of the patient be maintained as part of the patient's medical record, whether that record is paper or electronic. Online clinician-patient and clinician-clinician communications (including email) should be clinically-relevant as they are a permanent part of the medical record. [3]

4. Physicians should be aware of the following HIPAA Compliance issues:
   a. Physicians should ensure that online communications with patients are conducted over a secure network, with provisions for privacy and security, including encryption, in accordance with HIPAA. The use of standard email, such as Yahoo, AOL, or Gmail, to discuss sensitive patient information, may increase a physician's liability risk.
   b. Physicians should ensure that communication exchanged over social networking sites, including wall posts and pictures, complies with the standards set forth by HIPAA.
   c. Healthcare clinicians have responsibility for taking reasonable steps to authenticate the identity of correspondent(s) in electronic communication and to ensure that recipients of information are authorized to receive it. [2,3]

5. When communicating with patients on social networking sites, physicians should consider attaching a disclaimer that states that their responses do not represent formal medical advice and a board certified plastic surgeon should be consulted for a formal evaluation.

6. When interpreting and applying these principles to their individual practice, physicians should use their personal and professional judgment and, where appropriate, seek legal or other professional guidance. These principles are for general guidance only, and are not meant to serve as legal advice or a statement of any standard of care. This publication is provided with the understanding that the American Society of Plastic Surgeons is not engaged in rendering legal or other professional services.

References

[1] American Medical Association. (2010). "HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information" Retrieved from www.ama-assn.org/ama1/pub/upload/mm/368/hipaa-phi-encryption.pdf

[2] Federation of State Medical Boards, "Telemedicine Overview by State" (May 13, 2010). Retrieved from http://www.fsmb.org/pdf/GRPOL_Telemedicine_Licensure.pdf

[3] eRisk Working Group for Healthcare. (2006) "Guidelines for Online Communication".

Approved by the ASPS Executive Committee, September 2010