Advanced Technology and Confidentiality in Hand Surgery

Nash H. Naam, MD, Sandy Sanbar, MD, PhD

Advanced technology has the potential to improve the quality of care for our patients, but it also poses new challenges, especially in maintaining patient confidentiality. The Health Insurance Portability and Accountability Act and the newly enacted Health Information Technology for Economic and Clinical Health Act provide certain guidelines governing patients' medical record confidentiality. This article discusses the other new challenges facing hand surgeons, such as the use of social media, telemedicine, e-mails, and the Internet. *(J Hand Surg Am. 2015;40(1):182−187. Copyright © 2015 by the American Society for Surgery of the Hand. All rights reserved.)*

Key words Confidentiality, health, privacy, records, technology.

Hand surgeons, like other health care providers, must uphold the traditional moral precepts of patients' confidentiality, privacy, autonomy, self-determination, beneficence, nonmaleficence, and justice. They should place patient welfare above all other considerations; protect confidentiality and privacy; provide adequate patient informed consent (including the possible presence of other clinicians or trainees, photos, biopsy or scrapings being taken and stored, or telemedicine intervention); promote trust in the healing relationship; and ensure fair and equitable access to quality services cost-effectively. This article focuses on confidentiality and privacy in hand surgery in the modern era of rapidly advancing health information technology.

Health information technologies (HIT) strive to optimize the balance of risks and benefits to the patient, and augment the skills, shared trust, comfort, and compassion manifested by physicians, nurses, and other health care providers. When used ethically, HIT positively affects the lives and welfare of patients. Basic HIT includes telemedicine/telehealth, electronic medical (health) records (EMR), electronic clinical support systems, and on-line health care resources that market to health care providers and consumers. When using e-mail, telephone calls, videoconferencing, or other electronic means, one can never be completely sure who is gleaning information on the other end of the line, or even tapping into such information as it is being sent across the network. Physician should not disclose the patient's name or any other identifying information in any communication that is not encrypted. The best option is to obtain the patient's consent to sending such information.

From the Department of Plastic and Reconstructive Surgery, Southern Illinois University; the Southern Illinois Hand Center, Effingham, IL; and the Oklahoma University Health Sciences Center, Oklahoma City, OK.

Received for publication February 15, 2014; accepted in revised form March 13, 2014.

No benefits in any form have been received or will be received related directly or indirectly to the subject of this article.

Corresponding author: Nash H. Naam, MD, Department of Plastic and Reconstructive Surgery, Southern Illinois University, 901 Medical Park Drive, Suite 100, Effingham, IL 62401; e-mail: nnaam@handdocs.com.

0363-5023/15/4001-0034$36.00/0
http://dx.doi.org/10.1016/j.jhsa.2014.03.011

CONFIDENTIALITY

Information that is given by a patient to his or her medical provider must be kept confidential and will not be disclosed to anyone without the clear and unequivocal consent of that individual.[1] The Hippocratic Oath[2] that is sworn by new physicians as they start their practice states in part:

> Whatever in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.

> All that may come to my knowledge in the exercise of my profession or in daily commerce with me which ought not to be spread abroad, I will keep secret and will never reveal.

The American College of Surgeons adopted a more modern version, which states, "The surgeon should maintain the confidentiality of information from and about the patient, except as such information must be communicated for the patient's proper care or as is required by law."[3]

Once a physician–patient relationship is established or created contractually, a duty arises on the part of the physician to provide high standard medical care. The physician–patient relationship should be established on mutual trust and respect, which includes the certainty that all personal or medical information provided by the patient to the physician be kept strictly confidential.[4,5] This encourages patients to seek medical advice without fear or concern that their personal or medical information will be disseminated to anyone or any entity without their consent.[6] Unauthorized disclosure of confidential information has the potential of not only damaging that mutual trust between the physician and the patient, but also exposing the physician to possible legal implications.

Confidentiality covers the patient's information and the physician's opinions and conclusions based on the evaluation and assessment of the patient, including laboratory tests, x-rays, computed tomography scans, and so forth, and all communications between the patient and the physician and office staff.[6] The physician has the responsibility to educate the office staff on how to strictly maintain confidentiality of patients' medical records. The duty to maintain confidentiality persists even after the patient is no longer being treated by the physician.[7]

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

In 1996, the Health Insurance Portability and Accountability Act (HIPAA; also known as the Kennedy–Kassebaum Act) was enacted and signed by President William Jefferson "Bill" Clinton.[8] The Act addresses patients' right to confidentiality of medical information and to access health information despite changing jobs. It establishes policies, procedures, and guidelines for the protection and security of protected health information (PHI). The Health Insurance Portability and Accountability Act stipulates that every physician or health care provider must monitor employees' access to patients' private information. Protected health information can be disclosed without the patient's consent only for purposes of treatment, payment, or health care operations. Even in cases involving treatment, payment, or health care operations, the physician or the organization must follow clearly stated policies and applicable state and federal laws.[8,9] All other disclosures of PHI require written authorization signed by the patient. The Act requires the physician or the organization to take necessary steps to ensure confidentiality of communications with the patient. Importantly, HIPAA established a national standard for disclosure of PHI: namely, that a reasonable effort should be made by the provider to disclose only the minimum necessary information to achieve its purpose.[7]

In 2013, the Department of Health and Human Services published the HIPAA Omnibus Rule, which strengthens and amends existing regulations in the HIPAA Privacy and Security Rules.[10] The rule will significantly affect health technology and telehealth companies, data centers, and personal health record vendors. It expands the definition of business associates to include the following:

- Entities, such as data centers, that maintain protected health information (PHI) on behalf of covered entities;
- Health information organizations, e-prescribing gateways, and other entities that provide data transmission services for PHI to a covered entity and that require access to PHI on a routine basis;
- Entities that offer personal health records to individuals on behalf of a covered entity; and
- Subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate.

In addition, the Omnibus Rule increases liability for business associates making them directly liable for:

- Impermissible uses and disclosures;
- Failure to provide breach notification to the covered entity;
- Failure to provide access to a copy of PHI to either the covered entity, the individual, or the individual's designee;
- Failure to disclose PHI when required in an investigation of the business associate's compliance with HIPAA;
- Failure to describe when an individual's information is disclosed to others; and
- Failure to comply with the HIPAA Security Rule's requirements, such as performing a risk analysis, establishing a risk management program, and designating a security official, among other administrative, physical, and technical safeguards.