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.

Noncompliant business associates will be subject to civil monetary penalties ranging from $100 to $50,000 per violation, with the penalty for multiple violations of the same provision capped at $1.5 million. Physicians can be liable to the degree to which they have an authority over that business, so they must ensure that these businesses are in compliance with the law.

AMERICAN SOCIETY FOR SURGERY OF THE HAND

The Code of Ethics and Professionalism for Hand Care Professionals adopted by the American Society for Surgery of the Hand states, "The hand surgeon should respect the rights of patients, colleagues and other health professionals and must safeguard patients' health care information as mandated by law."[11,12]

Confidentiality of PHI is not always absolute.[7] There are 2 general situations that may compel the physician to disclose the patient's PHI without consent:

1. Concerns for the safety of the patient or others:
   a. Threat of self harm: If there is a good reason for the physician to suspect that there is a potential threat by the patient to himself or herself, the physician is legally and ethically justified to disclose confidential information to authorities.
   b. Threat to a specific person: It is the consensus of the law that if a physician has a reason to believe that a specific person or persons might be harmed by the patient, the physician has an obligation to make a reasonable effort to warn that individual or individuals. In *Tarasoff v Board of Regents of the University of California*, a psychologist and his employer were sued for failing to warn a woman that a man she had dated had expressed his intentions to kill her. When the woman was actually killed by that man, her parents sued for "failure to warn of the danger." The Supreme Court of California held that mental health professionals have a duty to protect individuals who are being threatened with bodily harm by a patient. The original 1974 decision mandated warning the threatened individual, but a 1976 rehearing of the case by the California Supreme Court called for a "duty to protect" the intended victim. The professional may discharge the duty in several ways, including notifying police, warning the intended victim, and/or taking other reasonable steps to protect the threatened individual.[13]
2. Concern for public safety:
   a. Communicable and infectious diseases: The state has an obligation to protect public health. That obligation sometimes outweighs patients' right to have their PHI protected. Some infectious diseases are reportable such as acquired immunodeficiency syndrome, human immunodeficiency virus, hepatitis A and B, measles, rabies, tetanus, and active tuberculosis.
   b. Specific injuries: Public health laws may require reporting of certain injuries such as gunshot wounds or any injury sustained in the course of a criminal offense, such as sexual assault.
   c. Suspected cases of child or elder abuse: There are laws in every state that require notification of authorities in cases of suspected child or elder abuse.

ADVANCED TECHNOLOGY

Advanced technology has the potential to improve the quality of care by facilitating instant access to PHI and faster exchange of health information by the providers who are involved in that patient's management. However, the use of advanced technology has introduced new challenges in maintaining the strict confidentiality of patients' medical information, thereby increasing the risk of unauthorized access and possible disclosure of PHI.[14–17]

To date, many health care facilities use EMR, in which health information is passed through computer systems and network links. Some medical records are kept in a so-called "cloud," which may easily be accessed or hacked. This has made the confidentiality process more difficult to maintain. Nevertheless, the physician remains responsible for ensuring the safety and confidentiality of patients' medical and personal information. Secure servers, computers, and file storage systems must be maintained and updated periodically to keep all the information safe and confidential.[16,17]

The physician should institute the following administrative, physical, and technical safeguards to protect patients' electronic protected health information (EPHI)[18]:

- Administrative safeguards are policies and procedures that demonstrate how the entity will comply with the law. The procedures should clearly identify employees who have access to EPHI. A contingency plan should be in place for responding to emergencies. The plan should document data priority and failure analysis, testing activities and charge control procedures.

- Physical safeguards indicate controlling physical access to protect against inappropriate access to protected data. Access to hardware and software must be limited to properly authorized individuals. Policies are required to address proper workstation use.
- Technical safeguards: Access must be controlled to computer systems and communications containing EPHI transmitted electronically over open networks must be protected from being intercepted by anyone other than the intended recipient. Information system housing EPHI must be protected from intrusion. When information is transmitted via open networks, a form of encryption must be used.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

As part of the American Recovery and Reinvestment Act, the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted to promote the adoption and meaningful use of HIT.[18] Subtitle D of HITECH addresses privacy and security concerns associated with the electronic transmission of health information, and specifies the measures that should be taken in case of a breach of EPHI.[16,18] Breach is defined as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information." A health care organization must notify every patient who might have been affected by a breach, by first-class mail.[19,20] If a hacker was able to gain access to a physician practice's computer system, laptop, tablet, smartphone, or other mobile or digital device that contained nonencrypted PHI, the physician may need to notify not only the patients, but also the Department of Health and Human Services, of the breach. Notification of a breach is not required if the data have been encrypted. The Act also requires that the encryption keys should be kept on a device separate from the data that they encrypt or decrypt.[20] Exemption from the breach notification requirements would be invalid if the encryption keys had been kept on the same device as the encrypted data. All PHI transmitted electronically should be encrypted, including practice management system, electronic medical records, scanned images, and any e-mails that may contain PHI. Penalties can be imposed against an individual within a health care organization, as well as the organization itself. Penalties could reach up to $1.5 million per violation.[18] This is in addition to any criminal penalties that might apply.

TELEMEDICINE

In telemedicine, breaches in confidentiality can be both visual and auditory. The unauthorized viewing of patient information of any kind—intentional or unintentional, whether written, electronic, or auditory—is unethical and typically not in compliance with the law or regulatory policies regarding privacy.[21,22]

Telemedicine is a clinical intervention that requires verbal or written informed consent from patients, or their representatives, similar to an office visit. The success of a telemedicine experience depends on establishing policies and procedures to ensure consistency, generalization, and quality; developing informational material for providers and patients; and providing community-wide education on PHI so that providers will respect privacy and confidentiality. Physicians and hospitals should also establish policy and procedures regarding the use of telemedicine, including patient education materials that clearly describe what one should expect during a telemedicine visit.

E-MAILS

Many physicians communicate with patients via e-mail. Increasing numbers of patients actually prefer to use e-mail to communicate with their physicians.[21,23,24] Hassol et al[25] found, in a large study of outpatient population, that patients prefer to use e-mail or on-line communications to obtain answers to general medical questions and routine follow-up for minor problems, but they prefer face-to-face discussion to discuss treatment options. Surprisingly, most patients were not concerned about the confidentiality of their information.[23,24] Although the law allows physicians to send PHI through unsecure e-mail, it is not recommended because the information could be breached by an unauthorized party. If physicians use unsecure e-mail to communicate with patients, they should consider seeking the patient's written consent.[21]

The Code of Medical Ethics of the American Medical Association outlines some guidelines for physicians regarding the use of e-mail[26]:

1. E-mail should not be used to establish a physician−patient relationship. E-mail could be used to supplement other more personal encounters.
2. When using e-mail for communication, the physician should hold the same ethical responsibilities as they do during person-to-person encounters.
3. Physician should inform the patient about the inherent limitations of e-mail, such as the potential of breach of confidentiality. Disclaimers cannot absolve the physician of the ethical responsibilities to protect patients' rights.

4. It is highly recommended to ask for the patient's consent to continue e-mail communications.

E-mails should not be used to convey bad news or abnormal or confusing test results, or to discuss treatment options that would require more person-to-person discussion.[27]

SOCIAL MEDIA

There has been a dramatic increase in the use of social media in the past few years. Some physicians use them for professional activities. Although social media can positively influence patient care, they have the potential to erode the level of confidentiality that physicians strive to achieve. In hand surgery practice, Lifchez et al[27] suggested that only general medical advice can be posted on social media outlets, but direct patient care should never be offered. Social media can be beneficial to both the physician through more exposure and the patient, who can gain useful information about medical conditions, but they should not be used to establish a physician–patient relationship.[27,28] The American Medical Association, Massachusetts Medical Society, and American Academy of Orthopedic Surgeons have published guidelines for physicians regarding the use of social media.[26,29,30]

INTERNET

Since its birth in the 1980s, the Internet has emerged as a powerful tool for interaction. In 2012, approximately 273 million people in North America used the Internet, which is about 80% of the population. Over the past decade, connections to the Internet became possible through small, mobile devices such as smartphones, tablets, and iPads. This has facilitated communication and access to information. There has been a marked increase in Internet use by patients and their families.[21,23,25] Patients search for information related to their condition. Physicians started using the Internet for patient education by posting medical information, videos, and images of medical conditions and procedures. Physicians should be careful before posting information on-line. The posted medical information should be general in nature and supported by scientific data. Any complex medical conditions should not be discussed on-line.[27]

When posting any information on-line, including images, x-rays, and videos, physicians should be certain that patients' confidential information is hidden. All uploaded material should be HIPPA-compliant. x-rays or other images should not contain identifying information about the patient.[17,18,21,25] Even images of hands can sometimes contain identifying information, such as tattoos.[27] The other alternative, which is always safer, is to obtain authorization from the patient to post the information on-line. If a physician needs to use a smartphone to transmit some patient information such as x-rays or laboratory results, it is important not to include identifying information. Again, it is always safer to ask patients' permission before sending their information via mobile devices.

CONCLUSIONS

- To enhance care when using EMR, it is the responsibility of physicians and agencies to: (a) create a common health record to facilitate the exchange of clinical information among health providers; (b) create regional governance structures to encourage the exchange of clinical data; and (c) initiate payment by purchasers of care, both public and private, to physicians for using electronic health records in both the rural clinic and tertiary hospital.[31] The conclusion represents "Golden Rules," which are inspirational goals for which to strive, to optimize the accessibility and confidentiality of medical information.
- To prevent HIT ethics conflicts, providers should (a) respect privacy and confidentiality in telemedicine and ensure adequate informed consent; (b) ensure accuracy of EMR, as well as accessibility and accountability by providers; and (c) seek information transferability between systems.
- When using electronic clinical support systems, ensure access and reliability of the decision support systems for local sites, and obtain support from tertiary care sites when needed.
- Finally, when accessing on-line health care resources, ensure the accuracy and reliability of information being accessed and encourage careful scrutiny by those accessing such information.

REFERENCES

1. Weiss BD. Confidentiality expectations of patients, physicians, and medical students. *JAMA*. 1982;247(19):2695–2697.
2. Jones E. *Hippocrates*. Vol. II. Cambridge, MA: Harvard University Press; 1923:297.
3. American College of Surgeons. Statement of principles. Available at: www.facs.org/fellows_info/statements/stonprin.html. Accessed December 5, 2013.
4. Rozmaryn LM. Decency, honor, integrity and the law. *J Hand Surg Am*. 2011;36(8):1397–1402.
5. Landrum SE. Patients' rights and responsibilities. *J Arkansas Med Soc*. 2003;99(7):222–223.
6. Rosenbaum S. Managed care and patients' rights. *JAMA*. 2003;289(7):906–907.

7. Jones JW, McCullough LB. Limits of confidentiality: to disclose or not to disclose. *J Vasc Surg*. 2013;58(2):521–523.
8. United States Department of Health and Human Services. The Health Insurance Portability and Accountability Act of 1996 (HIPPA) Privacy, Security and Breach Notification Rules. Available at: http://www.hhs.gov/ocr/privacy/. Accessed December 5, 2013.
9. Federal Register. Vol. 74, No. 209. Friday, October 30, 2009. Rules and regulations. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf. Accessed December 5, 2013.
10. United States Department of Health and Human Services. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/. Accessed December 5, 2013.
11. American Society for Surgery of the Hand. Code of Ethics and Professionalism for Hand Care Professionals. Available at: http://www.assh.org/Members/Ethics/Pages/CodeofEthics.aspx. Accessed December 5, 2013.
12. Rayan G, Glickel S. Ethics and professionalism for hand surgeons. *J Hand Surg Am*. 2010;35(9):1554–1555.
13. *Tarasoff v Regents of the University of California*. 17 Cal. 3d 425, 551 P.2d 334, 131 Cal. Rptr. 14 (Cal. 1976).
14. Bernat JL. Ethical and quality pitfalls in electronic health records. *Neurology*. 2013;80(11):1057–1061.
15. Wang CJ, Huang AT. Integrating technology into health care: what will it take? *JAMA*. 2012;307(6):569–570.
16. Sade RM. Breaches of health information: are electronic records different from paper records. *J Clin Ethics*. 2010;21(1):39–41.
17. Ferguson T. Digital doctoring—opportunities and challenges in electronic patient-physician communication. *JAMA*. 1998;280(15):1361–1362.
18. HITECH Act. Certification and EHR incentives. Available at: http://www.healthit.gov/policy-researchers-implementers/hitech-act-0. Accessed December 5, 2013.
19. Kim D, Schleiter K, Crigger BJ, et al. A physician's role following a breach of electronic health information. *J Clin Ethics*. 2010;21(1):30–35.
20. Hoffman S. Breach notification and the law. *J Clin Ethics*. 2010;21(1):42–43.
21. Blake JH, Schwemmer JD, Sade RM. The patient-surgeon relationship in the cyber era: communication and information. *Thorac Surg Clin*. 2012;22(4):531–538.
22. Rannefeld L. The doctor will e-mail you now: physician's use of telemedicine to treat patients over the Internet. *J Law Health*. 2004;19(1):75–105.
23. Gaylin DS, Moiduddin A, Mohamoud S, Lundeen K, Kelly JA. Public attitudes about health information technology, and its relationship to health care quality, costs, and privacy. *Health Services Res*. 2011;46(3):920–938.
24. Leong SL, Gingrich D, Lewis PR, Mauger DT, George JH. Enhancing doctor-patient communication using e-mail: a pilot study. *J Am Board Fam Pract*. 2005;18(3):180–188.
25. Hassol A, Walker JM, Kidder D, et al. Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. *J Am Med Inform Assoc*. 2004;11(6):505–513.
26. American Medical Association. Policy: Professionalism in the Use of Social Media. Available at: http://www.ama-assn.org/ama/pub/meeting/professionalism-social-media.shtml. Accessed December 5, 2013.
27. Lifchez SD, McKee DM, Raven RB, Shafritz AB, Tueting JL. Guidelines for Ethical and Professional Use of Social Media in a Hand Surgery Practice. *J Hand Surg Am*. 2005;30(5):2636–2641.
28. Rozental TD, George TM, Chacko AT. Social networking among upper extremity patients. *J Hand Surg Am*. 2010;35(5):819–823.
29. Massachusetts Medical Society. Social media guidelines for physicians. Available at: http://www.massmed.org/AM/Template.cfm?Section=Legal_and_Regulatory&Template=/CM/HTMLDisplay.cfm&ContentID=55132. Accessed December 5, 2013.
30. Soyer D. Social media in healthcare: a primer for orthopaedic surgeons. Available at: http://www3.aaos.org/member/prac_manag/Social_Media_Healthcare_Primer.pdf. Accessed December 5, 2013.
31. Fleming DA. Ethics conflicts in rural communities: health information technology. In: Nelson WA, ed. *Handbook for Rural Health Care Ethics: A Practical Guide for Professionals*. Hanover, NH: Dartmouth College Press; 2009:277–303.