ACUPUNCTURE Today

Confidentiality: What Is HIPAA? Part One

Fred Lerner, DC, PhD, FACO

I had the honor of becoming a United States citizen very recently. While going through the process, I learned a lot about how government works, how the United Sates was founded, and the Constitution and its amendments, as well as some authors of famous quotations, such as the person who said, "Give me liberty or give me death." (If you want the answer, it's at the end of this article.)

I bring this up because there have been some very significant changes regarding how health care practitioners protect their patients' privacy. The right to privacy is mentioned in many places in American law (and probably many other countries). The Fourth Amendment to the U.S. Constitution in particular guarantees that "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures shall not be violated."

This all has to do with every patient's right to privacy, or patient confidentiality. In the past, the rules were fairly simple. Charts did not get released or copied without a patient's written consent or by subpoena. Health care practitioners and their staff were bound by law not to reveal any health information to anyone. Even with a subpoena, many states specifically precluded the release of information relating to AIDS on a given patient without their specific written permission. This did not pertain to other reportable public health information; it also did not apply to law enforcement agencies.

This picture has been limited by technology in the past, but that has changed remarkably with computers, e-mail, the Internet, electronic claims submission, etc. There are several examples in which people lost jobs, bank loans, life insurance policies and were otherwise compromised because their medical records (and other private information) were easily accessible on the Internet. In many cases the information was incorrect, and the loss of livelihood and other important rights triggered a great deal of concern. While a few states had laws governing aspects of patient privacy, there was no national system in place, especially with the advent of electronic information sharing.

Congress and the President (in this case, Clinton) first passed the Medical Records Confidentiality Act of 1995 in an effort "to establish uniform privacy protection for personally identifiable health information." On one hand, patients now had access to any health information about them and gave people a chance to correct this information. In 1998, the Children's Online Privacy Protection Act was enacted to safeguard children online. There are many other examples building toward a national system.

A far more comprehensive strategy was passed in 1996, known as the Health Insurance Portability and Accountability Act, or HIPAA. The final ruling was released by the Department of Health and Human Services effective February 26, 2001, and health care providers (and other agents) are mandated to have it in place as of April 2003. The *Federal Register* describes HIPAA over about 700 pages. It can be downloaded off the Internet if you want to read it all, but I have attempted in this article to give you the "bare bones" as it relates to your practice.

HIPAA has three major purposes: (1) to protect and enhance the rights of consumers by providing

them access to their health information and controlling the inappropriate use of that information; (2) to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care; and (3) to improve the efficiency and effectiveness of heath care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

Who are the covered entities under HIPAA? Section 1172(a)(1) describes "health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction referred to in section 1173(a)(1) of the Act." If you read this far and are thinking that because you don't use electronic claims submission (ECS) you are exempt, think again. If any of the other entities (e.g., a health care plan) electronically submits your typed claim form, you are not exempt. In any event, I wouldn't plan on circumventing HIPAA. On principal, you have a duty to protect your patient's privacy.

The very first regulation deals with electronic transactions. The most common transaction of this type in most of our offices is electronic claims submission. Prior to ECS (and still used by many health care practitioners), health information was recorded and maintained on paper and stored in our offices. It usually took a physical exchange of these papers to breach confidentiality, or a verbal exchange of information. Today, most of this information is transmitted electronically, literally at the push of a button. In seconds, a person's very private information can be shared with anyone who can access it. The good news about electronic transmission is the increase in speed of delivery of effective care. In the practitioner's case, it isn't just about getting paid faster. The health information can be vital to that patient's life, for example, if they become hospitalized in a remote place and that information is needed. Obviously, there is a balance that must be maintained between safeguarding private information from abuse, fraud, prejudice and negligence, and sharing the same information for the patient's benefit.

Health information is often shared with consulting physicians. Let's say a patient is referred to you from a neurologist. That referral includes a diagnosis; possibly their MRI results; other diagnostic tests; and a phone conversation between the referring doctor and you. The referral information also may get disclosed to the health insurance company, managed care organization, employer (if it's Workers' Compensation), etc. How about getting a faxed MRI report or lab test? Much of the time, this is done without the patient's knowledge, but is innocently directed towards their benefit. Will this information delivery method change under HIPAA? Yes.

Failure to obey the HIPAA regulations will results in civil and criminal penalties, starting at $100 per person per violation and not exceeding $25,000 per year per person. The penalties get worse for knowingly violating HIPAA, especially if the offense is "under false pretenses," where there is a potential fine of up to $100,000 and/or imprisonment up to five years. They are much worse if the offense is with intent to sell a patient's information (up to $250,000 + 10 years imprisonment).

In part two, we will discuss specifics of how to comply with HIPAA. By the way, the author of "Give me liberty or give me death" was Patrick Henry. About one out of ten people I asked got that correct, so congratulations if you did.

FEBRUARY 2002