COMMENTARY

HIPAA the Health Care Hippo: Despite the Rhetoric, Is Privacy Still an Issue?

Kay Kuczynski and Patty Gibbs-Wahlberg

Patients have long been concerned about the privacy of their health care information. "How private is 'private'?" is a question that echoes through the minds of patients every time they receive a stigmatizing diagnosis such as cancer, a sexually transmitted disease (STD), alcohol or drug dependency, a mental or emotional health problem, or trauma symptoms related to a personal and private experience. Federal regulations for health care providers that went into effect in April 2003 are touted as improving or ensuring the privacy of an individual's personal health information, but do they? We think not.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L. 104-191) is a multitiered, comprehensive, convoluted, and controversial federal law for sweeping health care reform. Although HIPAA is dramatically broader in scope than privacy protections for health care information, a provision for privacy in the form of a Privacy Rule is included in Title II of HIPAA under the Administrative Simplification regulations; this regulation has created widespread controversy, as well it should, juxtaposed with both civil liberties and the tenets of our profession's ethical code.

In preparation for the Privacy Rule compliance date in April 2003, executives of covered entities (CEs), which include health plans, health care clearinghouses, and health care providers, were involuntarily plunged into a mire of federal definitions, acronyms, regulations, and procedures that spiked the jargon meter. A veritable compliance melee erupted as a result of struggles to comply with the letter of the law in the face of inability to decipher what the letter of the law was. A health care network-wide plethora of brochures, forms, and flyers, ostensibly aimed at protecting patient privacy better than ever before, spilled from the many months of compliance preparations by each CE. But contrary to the HIPAA hype about patient protection, and despite the glacier of paperwork for protecting privacy that was spawned by the Privacy Rule, critics of HIPAA claim that this federal law erodes patients' right to privacy. Citizens for Health filed papers in the U.S. district court in Philadelphia alleging that HIPAA regulations threaten "essential liberties [privacy] guaranteed by the Constitution" (Dougherty, 2003).

Privacy and confidentiality are in greater jeopardy than ever because of two security issues inherent in compliance with HIPAA regulations. The first security issue stems from the fact that health care providers are forced to use the Internet for sharing information and for billing purposes. Second, and counter to HIPAA's alleged intent, is the issue of access to private health information. According to a statement issued by Citizens for Health, "virtually all personal health information about every aspect of an individual's life can be used and disclosed routinely without notice, without the individual's consent and against his or her will" (Dougherty, 2003).

In the first instance, patient confidentiality is compromised by the federal government, health care workers, hackers, and the legal system. The federal government realizes a savings of billions of tax dollars by computerizing Medicare and Medicaid programs and HIPAA, and, except in very small practices, makes electronic billing mandatory. Also, to facilitate quick information exchange in medical emergencies, there is a push for universal patient identifiers, which relates to the second security issue. A nationwide linking of all medical records is possible with such identifiers (Gelman, Pollack, & Weiner, 1999). "A national health ID so presages a national health database that Congress has consistently refused to fund the program" (Privacilla.org, 2003, p.11). Even so, increasing amounts of new private health information will

CCC Code: 0037-8046/05 $3.00

be traveling the electronic highways, in addition to what is already stored in computers by managed care companies, as the private insurance companies follow the government's lead.

Managed care personnel have secured private health information about patients and clients to verify the necessity of treatment (Harris, 2003). During the past 15 years service providers assumed that this confidential information would remain safe with managed care personnel. With the retroactive element of the 2003 amendments to HIPAA, making past medical information available electronically, how valid is that assumption? Several years of paper treatment plans and client progress reports can be scanned into computer banks and be available for dissemination via the Internet. Internet use for insurance billing and sharing information is mandated by HIPAA, and the pesky problem of keeping that electronic information safe and secure is also addressed by HIPAA, allocating that responsibility to the service providers.

Unfortunately, that allocation does not guarantee that private medical information will remain safe and secure in storage or transit via the Internet. As distribution of information widens via the Internet, that information is more apt to become public (Aaronson, 2002). With date of birth, gender, and five-digit zip codes, 87 percent of the U.S. population can be identified (Aaronson).

"Instances of computer security breaches and associated financial losses have soared in recent years" (Raul, Volpe, & Meyer, 2001, p. 2). Computer programs now exist to crack passwords. In the first 20 minutes of an attempted break-in to a database, 20 percent to 50 percent of the Microsoft Windows passwords of a corporation with 10,000 employees could be found, and 90 percent could be found within 24 hours "by adding a brute force attack" (Lee, 2001, p. 2).

Hackers have enjoyed success in these endeavors. The confidential records of thousands of patients were stolen from the University of Washington Medical Center in 2001 (Chin, 2001), and in Philadelphia, Drexel University College of Medicine's database of 5,000 neurosurgery patients was accessed last year (Chin, 2003). Microsoft and the Pentagon, with state of the art computer security systems, were recently victims of hackers (Chin, 2001).

Computer security companies advertising the need for their products focus on the lack of security in cyberspace. Security lacks are documented by the Computer Security Institute and the FBI, which found in 2002 that 90 percent of large corporations and government agencies were victimized by hackers (Computer Security Institute, 2002). Doc-Shred (2003) estimated that "U.S. corporations are losing an estimated 100 billion dollars a year to information thieves" (p. 1). Prescriptions to remedy these situations include access-control servers, firewalls, intrusion detection, network scanning, encryption, and virtual private networks (Cisco Systems, 2001). However, as the hackers and computer security companies do battle, there is, to date, no foolproof system to keep Internet information 100 percent safe.

In addition to the problems of managed care's ownership and use of private medical information, the health care employee can compromise patient confidentiality through inadvertent errors. Electronic information can be sent to the wrong place, or the wrong information may be sent. The sheer volume of transmissions translates one simple mistake into thousands of cases misplaced or misdirected. Glitches occur within a "company's computer system leading to unintended dissemination of proprietary information" (Raul et al., 2001, p. 2). In August 2000, 858 Kaiser Permanente patients' confidentiality was breached when a computer glitch made incorrect appointments (Dyer, 2001).

In addition to negligent errors, people with access to medical information may have malevolent intent. A public health worker gave two newspapers a computer disk with 4,000 names of HIV-positive individuals. Medicaid clerks sold recipients' computerized printouts of financial resources to managed care companies. A banker called due the mortgages on cancer patients after cross-referencing information he obtained as a county health board member (Clark, 2001).

Legal recourse for damages caused by negligent failure to secure confidential information is woefully lacking. "To date no U.S. court has addressed the issue of liability for failure to secure a computer adequately" (Personick & Patterson, 2003, p. 45). The public has no recourse to sue under the new privacy rule (Peisert, 1999). HIPAA threatens penalties for noncompliance with security regulations, but if hackers or others obtain private information and an individual is harmed, suing in the courts does not seem to be an option. Rather, "if the right to refuse information sharing comes only from the

HIPAA privacy regulation, the consumer can only complain to the Department of Health and Human Services (HHS), getting in line behind thousands of other people to see if the agency will pursue his or her interests" (Privacilla.org, 2003, p. 23).

The second confidentiality problem under HIPAA is that information may be shared without the patient's consent and with the 2003 Amendments may be shared despite patient objections. Peter Kavanaugh (n.d.), past president of the Academy for the Study of the Psychoanalytic Arts, stated that the board of the Academy is opposed to the new

> HIPAA-cratic oath that requires the entry of personal and private information into a nationwide computer data base where it can be accessed by dozens of government agencies, thousands of bureaucrats, pharmaceutical corporations, private insurance companies, police agencies, foreign government officials and others . . . *without the person's consent*. (p. 2)

Health studies and drug marketing are instances in which patient data is shared (Aaronson, 2002). Law enforcement officials' access to patients' medical information has been broadened (Gelman et al., 1999). Public health activities may necessitate collecting individually identifiable information, including genetic information, without bothering to ask for an individual's consent (Peisert, 1999). Another broad area that allows sharing information without consent is defined only as having "specified public and public policy related purposes" (Richards, 2003). The FBI's new surveillance system could conceivably be used under these broad purposes. The new system was dubbed "'Carnivore' because it has the ability to get at the 'meat' of interesting or suspicious communications" (Lycos, 2003, p. 1).

The plaintiffs' brief, submitted to the United States District Court for the Eastern District of Pennsylvania by attorneys James C. Pyles and Kenneth I. Trujillo in *Citizens for Health v. Tommy G. Thompson, Secretary, U.S. Department of Health and Human Services,* clearly delineates the privacy concerns regarding the 2003 Amendments to HIPAA. The brief states that

1. "The Amendments eliminate their [citizens'] ability to exercise any control over the use and disclosure of their identifiable health information for routine purposes" (p. 3).
2. "Confer blanket federal authority on covered entities . . . to use and disclose their health information against their will and over their objections" (p. 3).
3. "Eliminate the ability to protect the privacy of their identifiable health information by paying out of pocket" (p. 5).
4. "Personal health information that they had permitted to be included in their medical records prior to April 14, 2003 would be used and disclosed without their permission" (p. 27).

Honorable Mary Ann McLaughlin entered a temporary order enjoining HHS Secretary Thompson's use of the Amended Privacy Rule "to the extent that it authorizes and permits the use and disclosure of Plaintiffs' identifiable health information without their consent" *(Citizens for Health v. Tommy G. Thompson)*. However, the final decision was favorable to the secretary of HHS.

In a news release on April 2, 2004, the secretary stated that the "court's decision supports our authority to protect the privacy of patient health information in a way that does not impede their access to quality health care. . . . We will continue to educate consumers about these important new protections and to promote compliance by those who, under the law, must safeguard patient health information." (HHS, 2004). Citizens for Health filed a Notice of Appeal on May 27, 2004. The Appellate Brief in this matter was filed on August 23, 2004 (Appeal for Patient Privacy Foundation, n.d.).

IMPLICATIONS FOR PRACTICE

The helping professions' focus regarding HIPAA has remained almost totally on compliance rather than questioning the impact of HIPAA on practice. Kavanaugh (n.d.) expressed concern when he wrote that "it seems that very little of these resources [time, money and effort] has been spent on critically assessing HIPAA's impact on the practice and profession of psychology" (p. 2). Germane to this assessment is whether we can preserve our clients' confidentiality, and there is a definite sense that we cannot.

As late as 2001, health information was difficult to obtain over the Internet because this information was being protected by "continuing practical obscurity" (Privacilla.org, 2003), that is, the existence of paper files and non-interchangeable electronic formats, then, as many as 400. As of 2004

transfer of information and Medicare and Medicaid insurance billing are required in compatible electronic formats.

As clients become cognizant that their private medical information can be accessed without their knowledge or permission, the trust implicit in the helping relationship could erode. Saxon (2001) explained that, unfortunately, "professional ethical standards are 'at the bottom'" (p. 14). Professions have no legal ground and must "give way to applicable constitutional, statutory or regulatory provisions" (p. 14). Regardless, the professions are compelled to act so that no harm is done.

Concerns about HIPAA and client confidentiality need to be raised by professional organizations so their members become aware of the possible impact of certain HIPAA regulations on their practices. Effort and time need to be focused on an assessment of the content and type of identifiable health information that is shared with managed care and insurance companies. Practitioners need to maintain case files (paper or electronic) that protect their clients from harm. Finally, time, energy, and money need to be directed to filing lawsuits in the federal courts, as in the case of *Citizens for Health v. Tommy Thompson,* to enjoin the HIPAA regulations that jeopardize the confidentiality of private medical information. SW

REFERENCES

Aaronson, T. (2002, November 27). *Bad medicine: Uncle Sam says a new law bolsters medical privacy.* Retrieved August 29, 2003, from http://www.vaccineinfo.net/issues/medicalprivacy/bad_medicine.shtml

Appeal for Patient Privacy Foundation. (n.d.). *The loss of medical privacy.* Retrieved March 30, 2005, from http://www.patientprivacyrights.org/

Chin, T. (2001, January 29). *Security breach: Hacker gets medical records. American Medical News.* Retrieved August 28, 2003, from http://www.ama-assn.org/amednews/2001/01/29/tesa0129.htm

Chin, T. (2003, April 7). Searchers may Google your patient records. *American Medical News.* Retrieved August 29, 2003, from http://www.ama-assn.org/amednews/2003/04/07/bisb0407.htm

Cisco Systems. (2001). *Network security solutions for health care: Making HIPAA SAFE.* Retrieved from www.cisco.com/go/offices/

Citizens for Health v. Tommy G. Thompson, Secretary, U.S. Department of Health and Human Services, U.S. District Court, Eastern District of Pennsylvania, No. 03-2267(MAM), dismissed April 2, 2004.

Clark, A. (2001, January 29). Security over the Internet. *Health Informatics Europe.* Retrieved August 29, 2003, from www.hi-europe.info/files/1998_9/security_over_internet.htm/

Computer Security Institute. (2002, April). *Cyber crime bleeds U.S. corporations, survey shows: Financial losses from attacks climb for third year in a row.* Retrieved March 31, 2005, from http://www.gocsi.com/press/20020407.jhtml?_requestid=652374

Doc-Shred. (2003). *On-site document destruction.* Retrieved August 28, 2003, from www.doc-shred.com/legislation.htm

Dougherty, J. (2003, September 6). Group sues feds over medical privacy: Doctors, patients, advocates claim new rules 'threaten essential liberties.' *World Net Daily.* Retrieved October 10, 2004, from http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=34450

Dyer, K. (2001). *The scope of medical informatics ethics.* Retrieved August 28, 2003, from http://www.journeyofhearts.org/jofh/jofh_old/minf_528/areas.htm

Gelman, S., Pollack D., & Weiner, A. (1999). Confidentiality of social work records in the computer age. *Social Work, 44,* 243–252.

Harris, E. (2003). HIPAA update: Resolving some areas of continuing confusion. Retrieved from http://www.masspsych.org/psychologist/research/masspsych/archived.html

Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191, 119 Stat. 1936.

Kavanaugh, P. B. (n.d.). *The new HIPAA-cratic oath for health care professionals.* Retrieved from http://www.mspp.net/acadnotes0603.htm

Lee, J. (2001, December 31). *Predictable passwords simplify a hacker's task.* New York Times Service. Retrieved September 10, 2003, from http://www.mail-archive.com/cybercrime-alerts@topica.com/msg00625.html/

Lycos. (2003). *'Carnivore' eats your privacy.* Retrieved September 3, 2003, from http://www.wired.com/news/politics/0,1283,37503.00htm/

Peisert, G. (1999, November 10). *Medical privacy alert.* Retrieved September 10, 2003, from http://lists.essential.org/noprivacy/msg00333.html/

Personick, S., & Patterson, C. (Eds.). (2003). *Critical information infrastructure protection and the law* (Open book). Washington, DC: National Academies Press. Retrieved August 28, 2003, from http://books.nap.edu/books/030908878X/html/

Privacilla.org. (2003, April). *The HIPAA privacy regulation—troubled process, troubling results.* Retrieved October 2, 2003, from http://www.privacilla.org/releases/HIPAA_Report.pdf

Raul, A., Volpe, F., & Meyer, G. (2001, August 8). Can hacking victims be held legally liable? *BNA Electronic Commerce Law Report, 6,* 849–858.

Richards, N. (2003, June 2). HIPAA and privacy: Who, what, where, when and why? *Health Innovation Daily.* Retrieved August 29, 2003, from http://health.innovationdaily.com/story_detail.html?story_id=133&section_id=6/

Saxon, J. (2001, May). Confidentiality and social services (Part II): Where do confidentiality rules come from? *Social Services, 31,* 12–15.

U.S. Department of Health and Human Services. (2004, April 2). *Statement by Tommy G. Thompson, Secretary of Health and Human Services regarding Citizens for Health v. Thompson decision on Privacy Rule* [News release]. Retrieved September 19, 2004, from http://www.hhs.gov/news/press/2004pres/20040402.html/

Kay Kuczynski, DSW, LCSW, *maintains a small private practice and is assistant professor, and* ***Patty Gibbs-Wahlberg*** *is program director and professor, Department of Social Work, East Tennessee State University, PO Box*

70645, Johnson City, TN 37614-0002. An earlier version of this commentary was presented at the annual conference of the Association of Baccalaureate Social Work Program Directors (BPD) November 1, 2003, Reno, NV. Address correspondence related to this commentary to Dr. Kay Kuczynski; e-mail: Kuczynski@etsu.edu.

Original manuscript received February 3, 2004
Final revision received October 18, 2004
Accepted January 10, 2005