

Social Workers and Post-Disaster Record Keeping Questions

Introduction

In the wake of Hurricane Katrina, social workers are reconsidering the methods for storing and destroying paper records, as well as whether or not to invest in electronic record-keeping solutions. Social workers who have not seriously considered these questions will find that the Health Insurance Portability and Accountability Act (HIPAA) standards for security of electronic records provide significant guidance in this area. This Legal Issue of the Month incorporates relevant HIPAA standards, and addresses such questions as:

- What is the best method of destroying paper records?
- Is there a national standard of practice regarding computerized records to replace paper medical records and the separate progress notes?
- Will computerized records be as valid in court, given the potential for amending them after the fact?

Document Destruction Options and HIPAA

There exists an industry of companies that specialize in secure, confidential document destruction and follow HIPAA standards. (Using an Internet search engine such as www.google.com and running a search on “confidential record shredding” will reveal a host of options.) Document storage and destruction companies are considered business associates of healthcare practitioners under HIPAA. They are required to sign a written business associate agreement wherein the company agrees to abide by certain HIPAA requirements in handling confidential health information (*U.S. Department of Health and Human Services*, 2002). NASW has sample business associate agreements available to members on its Web site. Companies that are in the business of document destruction will have a statement available regarding their compliance with HIPAA standards for medical privacy and security (see, for example, www.ironmountain.com).

Shredding is an accepted method of destroying clinical social work records (Houston-Vega & Nuehring, 1997). Healthcare practitioners who shred their own documents should use a “cross-cut” shredder, which reduces documents to the smallest pieces of shredded material. They may also want to explore pulverization methods.

HIPAA regulations provide standards for re-use and/or destruction of electronic media such as diskettes, flash drives, and other emerging storage technologies. Practitioners will want to develop a media re-use and destruction policy that specifies the circumstances in which electronic media can and cannot be re-used, and methods of destroying the data, such as the use of data “overwriting” software or physical destruction of the media.

National Standards for Electronic Record Keeping

At the time of this writing, no generally applicable requirement to keep electronic records exists at the national level. However, incentives are being developed that will make it increasingly difficult to avoid use of electronic health records. For example, the prompt

payment law in Missouri only applies to healthcare claims filed electronically (MO ST 376.384).

HIPAA generated a set of national regulatory standards that addresses privacy of both paper and electronic health records. These are federal requirements that apply to many, but not all, healthcare providers. There is no national "standard of practice" among the health professions regarding computerization of health records. However, there is a synergy of efforts among government agencies, the health information technology industry, healthcare insurers, and some healthcare provider groups to make this happen. For example, the U.S. Social Security Administration is implementing a process to transform disability claims into a completely electronic process using Electronic Medical Evidence (EME). Industry groups such as the Workgroup for Electronic Data Interchange, Strategic National Implementation Process (WEDI/SNIP) have been providing position papers and technical guides to assist participants in the process of creating and using electronic health records systems. Medicare requires healthcare providers, other than small practitioners, to file claims for reimbursement electronically.

Many healthcare practitioners still resist putting records in electronic format due to privacy concerns as to the ease of data transmission. Generally, the trend is towards computerization of health records; but many issues regarding how electronic health databases will be created and managed, the costs of computerization, and federalization of disparate state standards remain to be worked out.

Validity and Reliability of Electronic Records

Electronic records are already used as evidence in court for a wide variety of legal proceedings. Legal standards have been developed for the discovery or exchange of electronic business records in litigation. Under the HIPAA security standards, covered entities are required to put into place administrative, technical, and physical safeguards to assure that electronic health records cannot be improperly accessed or altered (NASW Legal Defense Fund, 2005). For example, access to computer systems containing electronic health records should be password protected. Records for closed cases can be saved in a "read-only" format, thus limiting the ability of any unauthorized personnel from making amendments to the record. The legal system is designed for the fact finders to review and weigh the sufficiency of the evidence presented. Use of electronic records presents an additional source of evidence, and the HIPAA standards may be raised for discussion when questions arise as to the validity of certain documents and the extent to which a particular electronic health record was properly secured.

Conclusions

An increasing number of social workers will need to be aware of HIPAA standards for security of electronic records and national healthcare industry trends toward the development of electronic health care records. Legislation under review in the current Congress proposes funding for the creation of healthcare databases.

A prudent social worker will want to develop a written clinical record destruction policy that outlines how long records will be kept and which records will be kept on-site; a log as to which records have been destroyed, the date, and the method; and provide the

method of destruction that adequately destroys all information, whether it is a paper or electronic record. Social workers who conduct electronic transactions with third-party payers will need to ensure that they comply with the HIPAA privacy and security standards, especially as new technologies emerge. Among the security standards are requirements for data back up and disaster planning and recovery plans for healthcare practitioners.

References

- Houston-Vega, M. & Nuehring, E. (1997). *Prudent practice: A guide for managing malpractice risk*, 46. Washington, DC: National Association of Social Workers. See also Morgan, S. & Polowy, C. (2001). *Social workers and clinical notes*. NASW Legal Defense Fund Law Note Series (p. 35, citing *Weathers v. Fulgenzi*, 884 P.2d 538, *543 (1994)). Washington, DC: National Association of Social Workers.
- Morgan, S. & Polowy, C. (2001). *Social workers and clinical notes*. NASW Legal Defense Fund Law Note Series. Washington, DC: National Association of Social Workers.
- National Association of Social Workers. (undated). *Sample HIPAA privacy forms and policies* [Online]. Retrieved from www.socialworkers.org/hipaa/sample.asp on November 18, 2005 (document is password protected for NASW members only). See also U.S. Department of Health and Human Services, Office for Civil Rights. *Sample business associate contract provisions* [Online]. Retrieved from <http://www.hhs.gov/ocr/hipaa/contractprov.html> on November 18, 2005.
- National Association of Social Workers. (1999). *NASW code of ethics*. Washington, DC: Author.
- National Association of Social Workers Legal Defense Fund.(2005, April). *Social workers and HIPAA security standards*. Legal Issue of the Month [Online]. Retrieved from http://www.socialworkers.org/ldf/legal_issue/200504.asp on November 18, 2005 (article is password protected for NASW members only).
- National Association of Social Workers Legal Defense Fund. (2005, October). *Social workers and record retention requirements*. Legal Issue of the Month [Online]. Retrieved from http://www.socialworkers.org/ldf/legal_issue/200510.asp on November 18, 2005 (article is password protected for NASW members only).
- U.S. Department of Health and Human Services. (2002, August 14). *Standards for privacy of individually identifiable health information: Final rule*. 45 CFR Parts 160 and 164. *Federal Register* 67, no. 157. §§ 164.502 (e)(1), 164.504.(e)(1) (Regulation Text, Unofficial Version, December 28, 2000 as amended: May 31, 2002, August 14, 2002, February 20, 2003, and April 17, 2003) [Online]. Retrieved from <http://www.hhs.gov/ocr/combinedregtext.pdf> on November 18, 2005.

*The information contained in this Web site is provided as a service to members and the social work community for educational and information purposes only and does not constitute legal advice. We provide timely information, but we make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in or linked to this Web site and its associated sites. Transmission of the information is not intended to create, and receipt does not constitute, a lawyer-client relationship between NASW, LDF, or the author(s) and you. NASW members and online readers should not act based on the information provided in the LDF Web site. Laws and court interpretations change frequently. Legal advice must be tailored to the specific facts and circumstances of a particular case. **Nothing reported herein should be used as a substitute for the advice of competent counsel.***