

New paperless technology and HIPAA: medical policy at the crossroads

Community Oncology recently published an excellent review of improvements in paperless record-keeping systems, covering everything from billing to scheduling to patient information (“Electronic medical records: taking the plunge,” March/April 2005, pp 157–168). However, patient privacy was not clearly addressed. Of concern is the vulnerability of such computer-based systems to intrusion, a concern shared by both the present administration and Congress.

President Bush himself has pushed for paperless medical records as a means of streamlining and perhaps reducing the cost of medical record-keeping. In 1996, Congress passed the Health Information Portability and Accountability Act (HIPAA), which was meant to keep patient information private—perhaps most importantly from the insurance industry, although everyone else is included in the law’s sweeping provisions. As a result, virtually every clinical office and department now have a paper shredder and a new sensitivity to patient privacy.

Who should have access to sensitive information?

There is another side to this technological revolution, however, that is often overlooked: Information passed over the Internet or even an office or hospital intranet can be improperly utilized by anyone, from those looking over one’s shoulder, to those who are less than absolutely secure in keeping their passwords to themselves, to those who appear to find new ways of hacking into almost anything. Primary access itself has become an issue. Should it be reserved for physicians alone or extended to nurses, secretaries, and even administrators? On raising the is-

sue with a local administrator regarding the range of accessible data on a new hospital system, her answer was, “Yes, it’s kind of scary.” It would appear she had access to patient medical records as well as billing information. In calling a doctor’s office when the doctor is out, one can learn that someone helpful, either a primary secretary or nurse, can readily access test results and other patient information off the computer.

Legend has it that Dr. Samuel Broder, the previous administrator of the National Cancer Institute (NCI), was offered the post as NCI head years ago in part because he had managed to keep AIDS information on an infamous patient from somehow escaping NCI’s computerized systems. These systems, whether hospital based or maintained by a large private medical group, are meant to be doctor friendly and are often available 24 hours a day, 7 days a week, every day of the year. I have personally called late at night, frazzled, trying to get access to a patient’s records in order to return a call from a patient who didn’t leave a number and wanted a test result. One can tell from the interaction that, unlike those at credit card companies or banks, the tech personnel are truly trying to help the caller. Frankly, though, it would appear to be easy to call with another doctor’s name and the same frazzled, earnest tone and gain access to a patient’s records. Likewise, I have been paged via the doctor’s internal paging system by non-physicians who are simply savvy about how hospital systems work.

Improper access is difficult to trace

Treatment records for everything from herpes to depression to cancer end up in databases. Were a member of the insurance industry found ac-

cessing such information, the penalties under HIPAA would be brisk indeed. But private individuals who hack into systems can store away information or twist it into a form that makes it difficult for law enforcement to prove anything. Using a computer and a wireless Internet connection in a café or some other anonymous site is difficult to track indeed. My 15½-year-old son has pulled things off the computer that left me hoping no one from the legal community would consider an innocent middle-aged doctor a witless fool. It has taken up to 8 hours to delete from my computer’s hard drive all manner of nonsense that my son discovered and downloaded from the time he was 12.

Locking the data away

Having now placed scientific data on a server, I’ve had to consider which files need to be secured from prying eyes. The information is stored in a locked room in an industrial-strength box for which only three people have a key. Each organization, be it a large private oncology group like US Oncology now embedded in a private fund, a hospital, or a hospital system, for profit or not-for-profit, will need to develop its own security for these precious, personal data. As for data that pass over the Internet, Michael Dell of PC manufacturing fame perhaps said it best: “Privacy? Forget about it!”

Thomas E. Goffman, MD, FACP
Departments of Radiation Oncology and
Microbiology and Molecular Cell Biology
Eastern Virginia Medical School
Norfolk, Virginia

We’d like to hear from you. Please send your instructive case reports, commentaries, and other brief communications to Randi Gould, Managing Editor, randi.gould@biolc.com.