June 5, 1997

# Patient privacy in peril

## Doctors struggle with security problem as more hospitals adopt systems / **Simson L. Garfinkel**

A FEW MONTHS AGO, A patient at the University of Washington Medical Center made what sounded like a reasonable request. Worried about his medical privacy, the patient asked that the hospital's computers be set up so his medical record could not be displayed on a computer terminal.

Today the UW Medical Center is still considering the request, but doctors aren't quite sure how to proceed. The college has been a leader in bringing computers to medicine, and there are few parts of the hospital that still rely on paper. Various computer systems at the hospital keep track of appointments, record procedures done, record laboratory work, send results to the physician, remind the patient when to schedule a follow-up, and, most important, send out bills. Precisely which computer does the patient not wish his information to be displayed upon?

"We're trying to figure that out right now," says one of the physicians on the hospital's medical informatics review panel.

So far there is no good answer.

Many physicians are increasingly worried that their age-old commitment to guarding the privacy of their patients is being jeopardized as hospitals adopt increasingly advanced medical information systems.

Earlier this year, the National Research Council issued a report on issues surrounding electronic health information. Called "For the Record," the report identified five "threat levels" for information stored in health care computers:

**Threat 1: Insiders making "innocent" mistakes that cause accidental disclosures of confidential information.** This could be as simple as a lab sending a fax to a wrong phone number, or a nurse pulling up one patient's medical records instead of another.

**Threat 2: Insiders abusing their access privileges.** Browsing seems to be a problem with many electronic record systems. The Internal Revenue Service, for example, has had persistent problems with curious employees looking through the tax records to which they have access. It's unreasonable to think that hospitals will somehow avoid this problem.

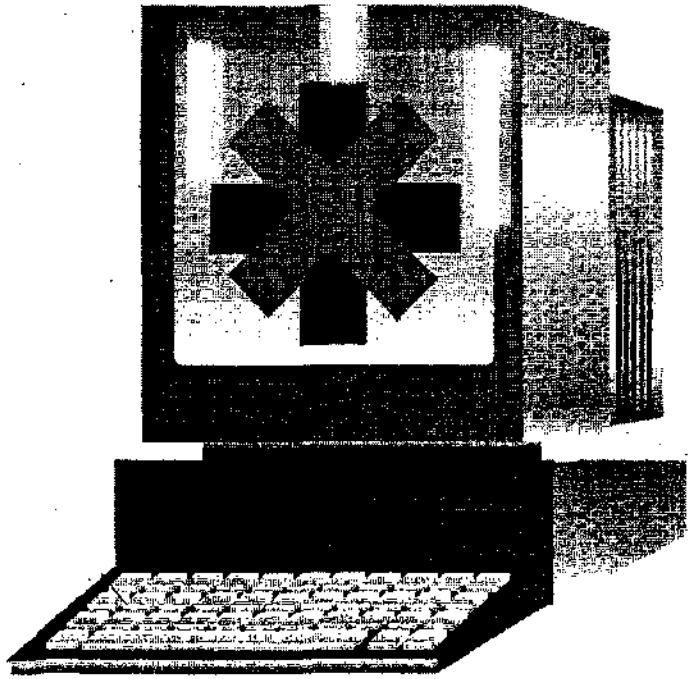
**Threat 3: Insiders who knowingly access information for spite or for profit.** During the 1992 Democratic primaries, a pathologist at Beth Israel said he was contacted by a member of the press who wanted access to Paul Tsongas's medical records. The reporter offered good money. A less ethical pathologist could easily have retrieved the file, probably without having that information traced back to him.

**Threat 4: An unauthorized physical intruder gains access to information.** Many hospitals rely on physical security to protect information stored inside a computer: The terminals are put in a special room or behind a desk to which only authorized personnel are supposed to have access. Unfortunately, hospitals are not as secure as hospital administrators would like to believe.

**Threat 5: Vengeful employees and outsiders, such as vindictive patients or intruders, who mount attacks to access unauthorized information, damage systems, and disrupt operations.** A doctor recently told me of a problem at her HMO: An employee has been accessing the HMO's scheduling computer and deleting patient appointments. The scheduling desk then thinks the appointment slot is free, and two or three patients show up at the same time.

The increased reliance on Social Security numbers is further compromising patient confidentiality. It is relatively easy to find out someone's Social Security number, and if you have it you can impersonate that individual, hunting down embarrassing or valuable pieces of medical information. What makes this scam possible is that many hospitals use Social Security numbers as a patient password.

Disturbingly, use of Social Security numbers by health care organizations is about to expand dramatically. Section 1173 of the Kennedy-Kassenbaum health care portability legislation passed last year defines a set of "administrative simplification procedures" that require the establishment of universal health identification numbers. The numbers will make it easier for organizations to combine data, both to improve patient care and to perform large-scale epidemiological studies.



It looks as if Congress or Health and Human Services will adopt the Social Security number as that universal identifier.

Some computer professionals suggest solving the health care privacy issue by encrypting all of a patient's files, so that the files can't be decrypted without his permission. The problem: It will make it difficult for doctors to access critical information at a time of urgent need.

Instead, many hospitals seem to prefer systems that allow relatively open access, but they record every file that's viewed or modified by every health care worker. The record is called an audit trail. The information can be used to find and punish employees who violate patient confidentiality.

But even audit trails break down in an emergency room, where forcing people to type a user name and password before ordering a test could mean the difference between life and death. Are you willing to die for your right to privacy?

Sometimes it is easy to forget that hospitals are turning to computers to lower costs and improve patient care. Unfortunately, ensuring patient privacy can be expensive and can prevent doctors from considering all of the pertinent data. It's doubtful we will be able to resolve the fundamental tension between the need to know and the need not to know.

---

*Technology writer Simson L. Garfinkel can be reached at plugged-in@simson.net.*