

## Are you ready for HIPAA?

### The Beast of Compliance Is Outside the Door; How Freaked Out Should Your Business Be?

by Michael Finley

Copyright 2002 by Michael Finley

Exclusively for *Twin Cities Business Monthly*

Need to understand why Congress passed a giant set of new standards for medical data? It can be explained in five quick vignettes:

#### #1 "The Sting Ray"

Vacationing in Florida, a strange sea creature bites you on the butt. Paramedics rush you to the hospital and pump you full of penicillin to ward off infection. Problem is, you're allergic to penicillin, but they can't tell that from your driver's license, so you die. Otherwise, it was a nice vacation.

#### #2 "Confidentially Speaking"

A hospital takes a call from a patient's wife. "I need copies of my husband's medical records," she says. The hospital complies. Months later, the husband sues the hospital, because he and his wife were getting a divorce at the time of the call. The information the hospital supplied was used to obtain a heftier settlement from the court.

#### #3 "A Janitor in Jamaica"

While vacuuming your hospital room, the maintenance man comes upon a chart on which appears your name, birth date, and Social Security number. Within 48 hours, he is ordering a double rum punch in Kingston town, and charging it to your credit card.

#### #4 "The Portability Problem"

You work for a blue chip telecom that abruptly declares bankruptcy and lays off all its employees, including you. Though you're a talented person, there's a small matter of a pre-existing health problem, a brain tumor requiring close supervision. Who will want to hire you now?

#### #5 "Talking in Tongues"

In olden times, XYZ Hospital wrote all its patient information on lined sheets and kept them in manila folders in file cabinets. Then along came electronic record-keeping, and a million vendors rushed in to provide programs and formats for maintaining patient info. A thousand such standards proliferated. Now no one at XYZ can talk to anyone outside XYZ.

## **HIPAA, hooray**

As the five anecdotes show, the old informal system of medical record-keeping hasn't kept pace with the technological and social changes our society has been going through. So Congress, in its wisdom, cobbled together in 1996 a comprehensive new set of healthcare laws with the weighty title Health Insurance Portability and Accountability Act, which we call by its nickname, HIPAA.

HIPAA mandates a major reengineering of the way we keep medical records. Consultants proclaim, not without glee, that it's "bigger than Y2K." How big, how major is it? The basic statute runs over a 1,000 pages, and weighs 22 pounds. The paradox? It's that all this volume and complexity is being applied to the task of "administrative simplification."

HIPAA covers an ocean of topics, including medical fraud and abuse, medical savings accounts, code sets, electronic signatures, state insurance pools, and of course portability of health benefits from job to job. Because of HIPAA, companies will have to reengineer organizational processes, retrain their entire workforce, alter their relationships with business partners, create a whole new consciousness in the heads of employees, and in the case of healthcare organizations, how providers deal with patients. But boiled down, three topics -- patient privacy, data security, and electronic transmissions of medical data -- are of critical interest to Minnesota businesses.

### **The patient's right to privacy**

First and foremost, HIPAA proclaims that the era of loosey-goosey data maintenance is over. No longer can a hospital post patient's names by their rooms. No more announcing patient's names on the public address system. No more diagnostic chart pegged to the wall by the patient's bed, telling all who pass by what she has.

Why the intensity about confidentiality? At the time HIPAA was drawn up, there was widespread fear that medical records could be shuffled about as unscrupulously as credit records. HIPAA is, in part, the response to that fear. It could be argued that it is an overreaction.

"In fact," said David Glaser, attorney with the firm of Fredrickson & Byron, "healthcare organizations have been pretty good about patient privacy. Common law provides good protection in most circumstances, and Minnesota state law anticipated the thrust of HIPAA. Doctors' offices and hospitals understood that privacy is important. In other words, from the patient's perspective, HIPAA won't change a whole lot."

But for other groups -- healthcare administrators, insurers, non-providers in the healthcare industry, and for employers in general -- HIPAA is an exasperating and expensive headache.

But HIPAA nevertheless constitutes a cultural change for many organizations. And it extends to non-healthcare companies, too. Peripheral device makers may not maintain files on patients by name. Even smaller companies that self-insure are finding that the cost of creating and maintaining HIPAA-safe benefits records is so great, that they are opting to move their health benefits to local PPOs.

"HIPAA effectively federalizes a matter that had previously been regulated on a state by state basis," said attorney Margo Struther of Oppenheimer Woollf & Donnelly. "It creates not a ceiling but a floor, a minimum requirement that may be superceded by existing state law. But it's important for organizations to learn about HIPAA now and be sure they get in on that ground level."

HIPAA is demanding, but not nonsensical. It permits doctors to informally solicit one another's opinions about cases. But it forbids them from talking about patients with people unrelated to the case. Doctors are to use common sense and discretion when discussing a case in a semi-private room, where other patients can overhear. But doctors do not need to soundproof their offices.

"The rules have lots of 'wiggle room,'" Glaser said. "In most cases they advise you to 'take reasonable steps.' The question you need to resolve in each case is what is reasonable."

Meanwhile, it isn't true that patients' medical records cannot be used against them. As the tale of the janitor in Jamaica illustrates, Minnesota is the number one state for identity theft. And the easiest way to steal someone's identification is to discover the two facts that patients traditionally enter first on their forms: their birth dates and Social Security numbers.

For this reason, all patient information online must now be protected with firewalls and access levels to prevent information from falling into the wrong hands. And all forms must be redesigned, with an eye to both standardization from place to place, and protection of patient privacy. And a new position must be created at most organizations, that of privacy officer, whose job it is to ensure that the structures of HIPAA are being followed.

It is a tremendous cultural change, not just for healthcare organizations, but for any organization that, for any reason, keeps records about patients -- including your company's health plan. And the change is costing everyone a ton of money.

"We have had tiny nonprofits come to us, and they can't believe the government is asking them to pay in the five figures to overhaul their records," said Roger Hughes of Data Security Auditors. But it is, and somehow or other, these small outfits are going to have to comply.

## **Battening the info-hatches**

HIPAA mandates that computer data containing information about patients must be safeguarded at every level, from the physical level (protection from fire, storms, and break-ins) to the virtual (protection from online attacks from hackers and viruses). None of this is news to most businesses. But many of us are still lackadaisical about security.

The most shocking statistic about data security may be that 99% of all wireless networks -- the handhelds and laptops so many providers use to beam their notes back to the server -- are unsecured, and vulnerable to attack and theft. Roger Hughes tells the tale:

"In the tests we conducted we discovered that nearly all wireless networks are not set up to be encrypted. Of the few that are encrypted, almost half use the password that comes

with the software, which is like no password at all. It's a huge hole that anyone can enter through."

Another huge hole is physical access. At many, many companies, an individual can enter a secured area merely by telling the guard posted outside, "Hey, I misplaced my access card -- would you be a pal and let me get to my desk?"

HIPAA advises us that our old excuses about slack security (using "password" as a password, leaving your machine up and running overnight) will no longer be tolerated.

### **Sidebar: Tips for improved data security**

These ideas are not explicit in HIPAA, but are good basic ways people in your organization can improve data security.

- Turn off your computer whenever you will not be using it for several hours.
- Scan with a current anti-virus program, frequently.
- Don't open unexpected email attachments.
- Don't let just anyone use your computer.
- Use secure passwords.
- Think twice before sharing, printing, or transferring your work with anyone.
- Make daily back-ups.
- Consider the security of sites to which you transfer data.
- Don't download software of unknown origin.
- Use a personal firewall if you maintain a medium to high amount of sensitive data on your system.
- If you access your work data from home use virtual private network software (VPN) to get a secure link.
- Before recycling or reselling old hardware, reformat the hard drive to delete sensitive data.
- If you notice anything "funny" about your computer or data, run, don't walk, to your network administrator.

### **Transmitting through hyperspace**

HIPAA came into being in 1996 just as the Internet began to mushroom. Lawmakers, led by Sens. Ted Kennedy (D-Mass.) and Nancy Kassebaum (R-Kan.) saw that online data sharing through intranets and websites would result in a Babel of proprietary electronic data interchange (EDI) standards. HIPAA's decree that all organizations adopt a common EDI standard acquired enormous implications for organizational IT.

George McNulty, president of Twin Cities technology consultancy Caveo Technology, says the IT impact of HIPAA is only a part of the law -- but it's an expensive one. "It threatens the financial stability of many healthcare organizations, especially those already on shaky ground, like most hospitals.

"And compliance isn't understood very well. Most healthcare organizations are relying on their software vendors for EDI solutions. But only 14% have any kind of credible, detailed plan for achieving EDI compliance. Many of the remaining 86% haven't even asked. They need to understand that HIPAA compliance will probably cost at least 1.5 times to achieve as the cost of Y2K compliance. It's that big."

### Sidebar: How much will HIPAA cost you?

Estimated compliance costs for different kinds of organizations.

| Organization Type       | Annual Revenues | Estimated Compliance Costs |
|-------------------------|-----------------|----------------------------|
| Health Plans            | \$250M-\$500M   | \$700,000                  |
| Hospitals               | \$250M-\$500M   | \$4,390,000                |
| Group Medical Practices | \$100M-\$250M   | \$116,667                  |
| Payers (Employers)      | \$100M-\$250    | \$1,088,750                |

Source: The Gartner Group

### Who wins, who loses

Ross Janssen, head of the office for HIPAA compliance at the University of Minnesota's Academic Health Center, has been at the eye of the storm for over a year now. The complexity of the University, plus the intricacies of HIPAA, have made it a daunting challenge.

"It's very difficult to know and understand all the business processes in all of the various entities. The information gathering process is massive, and requires cooperation and support of high level management. To complicate matters further, the regulations aren't finalized yet, so we have the task of trying to develop a plan to train students, staff, and faculty about regulations that we're not even sure of yet."

What's the best thing about the job? "Probably that we don't really have a choice about compliance. Since we've got to do it, there's been very little resistance."

Meanwhile, he said, there are obvious pluses. "The biggest benefit will be the cost savings associated with the implementation of the standard transactions and code sets. Everyone stands to benefit from that savings."