

THE NEW THREAT TO YOUR

MEDICAL PRIVACY

A national system of electronic medical records could easily save your life. And it could also jeopardize the security of your personal health information.

Let's say you have a heart attack. You could be swooshing down the water slide at Walt Disney World's Typhoon Lagoon, teeing off at the 16th hole at Pebble Beach, or raking leaves in your backyard.

Your odds of survival would soar because the emergency-room computer would let the doctor on duty connect to the Internet, type in a password, and with a few clicks, view your medical history. He could see your most recent test and lab results, a list of your allergies, and all your medications. With all that information, he could begin treating you immediately.

That scenario is not science fiction. The federal government is fostering the creation of a national system of electronic health records (EHRs) under the leadership of David Brailer, a 46-year-old physician and former software company CEO who is now at the U.S. Department of Health and Human Services. His charge: to help build the National Health Information Network, which will electronically connect all patients' records to health-care providers, insurers, pharmacies, labs, and claims processors by 2009.

The network's potential to save money, to make medical care more efficient, and to lower the incidence of deadly drug reactions and interactions

has spurred state government agencies, foundations, HMOs, PPOs, and hospital chains to develop their own electronic records systems, some of which are already up and running. "Electronic health records will reengineer health care in a way that will save thousands of lives and billions of dollars," Brailer says.

But troubling questions come with the promises. Will such private information be safeguarded from marketers who

might want to sell you a new drug to treat your asthma, or from fund-raisers who target you because the diagnosis of your new disease diagnosis might encourage you to contribute?

Could computer hackers or pranksters release the information onto the Internet, where your co-workers could learn, say, that you are being treated for alcoholism? Might your record become available to potential employers or lenders who decide that you're not healthy enough to perform the job or handle a 30-year mortgage? And will you be able to control who has access to or find out who has viewed your medical records?

Brailer says that consumers will be able to see their records and correct errors (assuming that they can decipher the medical gobbledegook). But the cost to consumers remains unclear. Brailer initially told us that consumers will pay an access fee. But he later said that access would be free. Jim Pyles, a Washington, D.C., constitutional lawyer and privacy expert, objects. "There is no reason there should be access to your records without your consent unless required by law or your life is in jeopardy," he says, "and you certainly should not have to pay for access to your own information."

FROM FOLDERS TO NETWORKS

Spread among folders at the offices of maybe a half-dozen doctors and possibly

CR QuickTake

The federal government, states, HMOs, and PPOs are developing a system to store and link the medical records of every American. The network would allow medical providers and insurers, among others, to view records and enter information. The ramifications:

- Doctors could provide better care by instantly viewing medical histories.
- The network could save money by eliminating duplicate tests.
- Health officials could quickly spot adverse drug reactions and epidemics.
- But marketers could target patients with specific diseases to sell them drugs or to solicit for related charities.
- In the absence of safeguards, lenders and employers could use medical records to disqualify people with health problems from obtaining loans and jobs.

hospitals, the traditional paper medical record is not necessarily efficient, secure, or accurate. Employees certainly and visitors sometimes have access to the folder-lined walls where many physicians keep their patient data. Charts may be misfiled, pages can fall out, and a spilled latte can wipe out years of data.

In recognition of the problems, medical institutions over the years have turned to computerization to manage patient information. At first these systems weren't connected. But gradually, large health-care providers, including the Department of Defense, the Department of Veterans Affairs, and managed-care companies, each linked individual office computers to form integrated systems that would allow health-care workers to retrieve patients' test results, including blood work, radiology, and biopsy reports.

After 9/11, federal officials recognized that a national system of interconnected records could help them spot early evidence of biochemical attacks and epidemics. "It takes 26 days for our current fragmented system to process data at the local level, then the state level, and have it

rise to the level of concern to reach the Centers for Disease Control and be properly analyzed," Brailer says. "In a fully integrated national system, problems can be spotted in a day."

To have all records connected to a nationwide system, providers, insurers, pharmacies, and other health-care entities will have to pay some \$150 billion over the next five years. "It can cost up to \$35,000 per doctor to get a fully integrated system in place," says Peter Waegemann, CEO of the Medical Records Institute (MRI), a group that has promoted the establishment of electronic health records. And, according to Brailer, some of the costs will eventually be passed on to consumers.

MRI's database contains 2,500 software and hardware suppliers. Some of them sell systems that support large provider chains. Others peddle specialty programs, such as ones tailored to dentists. "The problem is that most of these systems are not compatible, so they can't communicate," Waegemann says. "We need standards to be implemented or else the whole system could collapse."

THE PROMISES

So far, the development of medical information networks has been sporadic, but those in operation are already offering advantages to both doctors and patients. The VA has one of the few systems in place. Two physicians at the Veterans Affairs Medical Center in Washington, D.C., showed us how a patient's computerized record gives them access to layers of information, including notes from office visits, hospital admissions and discharge notes, special patient problems, allergies, diagnostic test results, and a list of the patient's medications.

Alerts signal the doctor if the patient is due for a test or procedure. With a click, test results fill the screen, including CAT scans, MRIs, and EKGs. Some of the images appear in 3D and can be rotated for a 360-degree view. A doctor at any of the VA's 1,300 care-center locations across the nation can pull up a patient's file and add information to it if a veteran is treated at that facility.

The system gives patients control over their medical care. Two Web sites called My HealtheVet—one of them a pilot with

you need to know

WHAT RIGHTS YOU ARE SIGNING AWAY AT THE DOCTOR'S OFFICE

Chances are that in the last few years, you've been asked to endorse dozens of so-called privacy agreements while sitting in doctors' waiting rooms. Under the provisions of the Health Insurance Portability and Accountability Act (HIPAA), health-care providers have the right to share your data for several purposes: to treat you, which means, for example, they may discuss your case and send data about you to a radiologist about which ankle to X-ray; to process your insurance claim; and to respond to requests from public-health authorities, law enforcement, and your employer if you were hurt at work.

All of that seems reasonable, but you might not realize that HIPAA also allows health-care providers to share information with health-care business associates. So notes from your psychotherapy session may be given to your insurers' employees for "training purposes." And don't forget about fund-raisers. For example, the agreement of Michael Bermant, a plastic surgeon in Chester, Va., says, "We may use or disclose your demographic information and the dates that you received treatment from us in order to contact you for fund-raising activities supported by our office."

Unfortunately, HIPAA does not give you the right to opt out in most cases, and the agreements can change at any time. But there

are ways to guard the shreds that are left of your medical privacy:

- Read notices of privacy practices carefully. If you do not understand something in the notice, ask questions. Your doctor may agree to keep personal or very embarrassing information out of your record as long as its absence will not negatively affect the quality of your care or your health.
- You do not have to sign the forms. Unfortunately, refusing to do so will not change the offices' ability to share your information. The notice is not a contract; it is merely a mandated disclosure form to prove that you were informed in writing about how your data may be shared.
- HIPAA gives you the right to request that your health-care provider or your health plan restrict uses or disclosures of your medical information. For example, you may say that you do not wish to receive fund-raising materials, a right that is noted in Bermant's notice. The provider or plan, however, is not obligated to agree to the restriction, which Bermant's agreement also notes. But if the provider or plan does agree to the restriction, which Bermant's office says it does, it must abide by that agreement, except in emergencies. Your request will probably have to be made in writing. The provider's or plan's office will then let you know whether it has decided to abide by your wishes.



more features—allow some 155,000 participating patients to have instant access to some of their medical records. Using an Internet connection, they can read their doctor's summary of a visit, see test and lab results the day after they come in, and type in any data they want to track on their own, such as blood-sugar level, blood pressure, or weight.

More precise patient care from doctors, greater participation by patients, and an early-warning system for medical disasters such as the appearance of avian flu are the hopes for an electronic records network. Another is the potential savings in health-care expenditures, which reached \$1.9 trillion in 2004.

According to a RAND Corporation study published in September, successful adoption of health-information technology by 90 percent of doctors and hospitals would cut health-care spending by \$77 billion annually. The biggest savings would come partly from shorter hospital stays prompted by better-coordinated care and fewer redundant tests and procedures. Fewer prescription errors, another benefit of computerized systems' warning doctors and pharmacists of potential adverse drug reactions, could shave off \$4 billion.

ERRORS ACROSS THE INTERNET

Anyone who has recently examined his or her credit report knows that errors are common and often significant. Errors in a medical record could be fatal.

It's axiomatic that paper records have errors. But the records don't have much reach. An error in your EHR, however, that says you have a possibly stigmatizing condition (depression, addiction, a sexually transmitted disease) can be seen by many people before you even know of the error.

The likelihood of errors could also increase when lots of people have the ability to enter data. John Halamka, a physician and chairman of the Healthcare Information Technology Standards Panel, whose job it is to set data standards for exchange of information over the network, insists that security will be tight. Each local network would require that individuals logging into the system have unique IDs tied to a designation such as R.N. or M.D. A patient's information would

Taking charge of his health

WHO Orlando Sellers, 57, a Vietnam War vet and a human-resources specialist at the Veterans Affairs Medical Center in Washington, D.C.

WHAT Sellers can pull up his electronic medical record at MyHealthVet, a Web site, and enter his daily blood-pressure reading. If he sees that it's spiking, he can send an e-mail note to his doctor, who may then ask him to come in for a brief checkup. (Sellers' doctor also checks his daily blood-pressure entries.)

Sellers takes comfort in the fact that doctors at any of the VA's 1,300 U.S. care centers can view his record even if he is unconscious and rushed to an emergency room. "It's like having luggage that you take on a trip that can save your life," he says.



WHAT THEY SEE Veterans Affairs patients view the basic information in their record, but doctors get much greater detail. The charts below show the difference between their views of blood-pressure readings.

PATIENTS' VIEW



DOCTORS' VIEW



be divided into subsets so that the dentist's nurse would be unable to view or alter the diagnosis of your psychiatrist. Or gossip about it to neighbors.

Without such safeguards, some consumers might be reluctant to seek treatment for certain conditions out of fear of discovery. "No one wants strangers to see the details of things like their cancer treatments, or their parent's sexual dysfunction, or their child's diagnosis by a therapist," says Deborah Peel, M.D., a psychoanalyst in Austin, Texas, and president of Patient Privacy Rights, a nonprofit medical-privacy watchdog group.

EYES ON YOUR RECORDS

As things stand now, HIPAA regulations allow your medical information to be shared by hundreds of thousands of people without your knowledge—to treat you and to process billing. But the data can also go to health-care-related businesses. "Medical ethics have always allowed doctors to share information about you with your consent to ensure you are properly treated and to process insurance claims," says Pyles, the privacy expert. "It's that third category, sharing with health-care-related businesses, that's troublesome." Troublesome because there are

Taking charge of others' health

600,000 health-care-related companies in the U.S., according to estimates by the Department of Health and Human Services (HHS), including drugmakers, fund-raisers, health-care researchers, law practices, law enforcement, marketing companies, and transcription services. And those businesses can share your data with their affiliates.

"That could total over a million firms, and there is no requirement in the rule that says you have to be notified when your record is shared with them," Pyles says. HHS estimated that obtaining your consent every time your data were shared could cost \$103 million over 10 years.

Your information could also be included in health-care research or public-health programs without your knowledge. Even if you find out about the research and request that your data not be included, the public-health organization is not required to acquiesce.

In January, for example, the New York City Department of Health began a program to monitor the blood-test results of more than 500,000 diabetic city residents. Labs are required to send test results electronically to the department, which analyzes them to identify people who are having trouble managing the disease. Patients are unable to have results excluded.

Patients deemed at risk may receive letters or phone calls from physicians urging them to take their medication, get more frequent checkups, or alter their diet; patients can, however, opt out of the intervention portion of the program.

Although many companies might already have access to your data, a network of electronic records has the potential to spread it much farther at a more rapid rate. "It's a lot harder to share information that's sitting in paper files in lots of different doctor's offices now," Peel says.

The HIPAA law allows data to be shared with health-care businesses, and privacy advocates worry that an electronic system could allow your insurer to share data about you with its affiliate, which could be your bank, which in turn may be doing some health-care consulting. Your employer may obtain your info if it is an affiliate of a health insurer or if it self-insures. And note that any negative re-

WHO Lynn Silver, the assistant commissioner for chronic-disease prevention and control at the New York City Department of Health.

WHAT New York's health department monitors the diabetes-test results of city residents without their consent. "Diabetes has reached epidemic proportions in the city, and this step will help us reduce many unnecessary deaths," Silver says. Currently, some 1,900 people die from diabetes-related complications in the city every year. The program monitors patients' conditions and contacts their doctors if it concludes they are having difficulty managing their illness.



sults of an employer-sponsored physical or test are not adequately protected information under HIPAA.

A corporation that is considering acquiring a pharmacy group or insurance company will be able to view its members' records as part of its due diligence. Data warehouses that process prescription data for pharmacies may share information with drugmakers about who takes which medicines to improve marketing.

The information may include your name, a diagnosis code, and the amount you paid, for example, but that could be enough to derail your prospects for a loan or a job. "You could be charged higher loan rates or lose a job because of what's in your medical record," Pyles says. "And it will be impossible to prove it was because your data was shared, rightly or wrongly, because there is no disclosure audit."

SAFEGUARDING AGAINST THEFT

Brailer and other network advocates say that the system will have the tightest possible security. But recent large-scale thefts of credit-card and banking information have shown that all databases, even those with state-of-the-art security protections, can be compromised.

Electronic health systems now in operation have already sprung some serious security leaks. In October 2003, for example, a medical transcriptionist in Pakistan threatened to post patient records from the University of California

at San Francisco's Medical Center on the Internet unless she was paid for her work for a transcription service hired by the university. The service was forbidden by its contract with the university to divulge contents of the recording or transcriptions. But that transcription service had subcontracted to another U.S. company, which in turn subcontracted to a firm that farmed the work out to Pakistan. Luckily, a UCSF official says, the woman relented and promised to destroy the records. UCSF fired its service. Patients, in the meantime, had no idea their records were being sent overseas.

In another breach, two computers and a disc containing the confidential records of close to 200,000 patients of a medical group in San Jose, Calif., were posted for sale on Craigslist.org, a classified-advertising Web site. The disc included a wealth of data, including names, dates of birth, Social Security numbers, insurance information, addresses, bill records, and medical histories. A former branch manager for the medical group was charged in May 2005 with the theft. At press time, he had not yet entered a plea. The public defender representing him did not return our calls.

The Federal Bureau of Investigation recovered the equipment and software, and the medical group informed current and former patients of the theft. It's not clear what a buyer would do with the information, but the medical group says that it has received no complaints from patients.