December 3, 2006

Health Hazard: Computers Spilling Your History

By MILT FREUDENHEIM and ROBERT PEAR

BILL CLINTON’S identity was hidden behind a false name when he went to NewYork-Presbyterian Hospital two years ago for heart surgery, but that didn’t stop computer hackers, including people working at the hospital, from trying to get a peek at the electronic records of his medical charts.

The same hospital thwarted 1,500 unauthorized attempts by its own employees to look at the patient records of a famous local athlete, said J. David Liss, a vice president at NewYork-Presbyterian.

And just last September, the New York City public hospital system said that dozens of workers at one of its Brooklyn medical centers, including doctors and nurses, technicians and clerks, had improperly looked at the computerized medical records of Nixzmary Brown, a 7-year-old who prosecutors say was beaten to death by her stepfather last winter.

Powerful forces are lobbying hard for government and private programs that could push the nation’s costly and inefficient health care system into the computer age. President Bush strongly favors more use of health information technology. Health insurance and medical device companies are eager supporters, not to mention technology companies like I.B.M. and Google. Furthermore, Intel and Wal-Mart Stores have both said they intend to announce plans this week to embrace electronic health records for their employees.

Others may soon follow. Bills to speed the adoption of information technology by hospitals and doctors have passed both chambers of Congress.

But the legislation has bogged down, largely because of differences over how to balance the health care industry’s interest in efficiently collecting, studying and using data with privacy concerns for tens of millions of ordinary Americans — not just celebrities and victims of crime.

Advocates of such legislation, including Representative Joe L. Barton, the Texas Republican who is the chairman of the House Energy and Commerce Committee, said that concern about snooping should not freeze progress on adopting technology that could save money and improve care.

“Privacy is an important issue,” said Mr. Barton, who will lose the chairman’s post when the Democrats take over next year, “but more important is that we get a health information system in place.” Congress can address privacy later “if we need to,” he said.

Democrats, however, have made it clear that they are determined to address the issue of medical-records privacy once they take command of both houses of Congress next month. “There is going to be much more emphasis placed upon privacy protections in the next two years than we have seen in the last 12 years,” said
Representative Edward J. Markey, Democrat of Massachusetts and a longtime privacy advocate.

Mr. Markey, a member of the Energy and Commerce committee, said he supported legislation that would allow individuals to keep their medical records out of electronic databases, and require health care providers to notify patients when health information is “lost, stolen or used for an unauthorized purpose.”

Representative John D. Dingell of Michigan, the ranking Democrat who is expected to become chairman of the Energy and Commerce committee next month, said that expanding electronic health care systems “clearly has great potential benefit.” But he added that “it also poses serious threats to patients’ privacy by creating greater amounts of personal information susceptible to thieves, rascals, rogues and unauthorized users.” Members of his committee, as well as the House Ways and Means Committee, have been struggling with such issues.

Academic medical centers like NewYork-Presbyterian have considerable experience with electronic records. But many other hospitals have been slow to jump on board, as have doctors and patients. Only one in four doctors used electronic health records in 2005, according to a recent study by researchers at Massachusetts General Hospital and George Washington University, and fewer than 1 in 10 doctors used the technology for important tasks like prescribing drugs, ordering tests and making treatment decisions.

Cathy Schoen, a senior researcher at the Commonwealth Fund, a nonprofit foundation, said primary-care doctors in the United States were far less likely than doctors in other industrialized countries to use electronic records. In Britain, 89 percent of doctors use them, according to a recent report in the online edition of the journal Health Affairs; in the Netherlands, 98 percent do.

Technology experts have many explanations for the slow adoption of the technology in the United States, including the high initial cost of the equipment, difficulties in communicating among competing systems and fear of lawsuits against hospitals and doctors that share data.

But the toughest challenge may be a human one: acute public concern about security breaches and identity theft. Even when employers pay workers to set up computerized personal health records, many bridle, fearing private information will fall into the wrong hands and be used against them.

“When I talk to employees, the top concern they have is: ‘What happens to my information? What about the Social Security numbers on my employee insurance, as well as the identity threat now appearing in health care?’ ” Harriett P. Pearson, I.B.M.’s chief privacy officer, said in a recent interview. “We have to be proactive about addressing privacy issues.”

Dr. J. Brent Pawlecki, associate medical director at Pitney Bowes, the business services company, said that people in the United States are most concerned that they could lose their health insurance, based on something in their health records. Pitney Bowes is weighing the pros and cons of electronic personal health records for its employees.

The worries are widely held. Most Americans say they are concerned that an employer might use their health insurance records to limit job opportunities, according to several surveys, including a recent one by the nonprofit Markle Foundation.
Some patients are so fearful that they make risky decisions about their health. One in eight respondents in a survey last fall by the California HealthCare Foundation said they had tried to hide a medical problem by using tactics like skipping a prescribed test or asking the doctor to “fudge a diagnosis.”

Dr. Stephen J. Walsh, a psychiatrist and former president of the San Francisco Medical Society, said, “I see many patients who don’t want any information about their seeing a psychiatrist on a record anywhere.”

CONGRESS addressed some of these concerns in 1996, when it passed the Health Insurance Portability and Accountability Act. That made it a federal crime, albeit rarely punished, to disclose private medical information improperly.

But critics say that the law has some worrisome loopholes, that infractions are rarely prosecuted, and that violators have almost never been punished. The law, for example, lets company representatives review employees’ medical records in order to process health insurance claims.

Critics say that it would not be unusual in some companies for the same supervisor to be in charge both of insurance claims and of hiring and firing decisions; this could allow companies to comb their ranks for people with expensive illnesses and find some reason to fire them as a way to keep health costs under control. Easily accessible computerized files would make the job that much easier, the critics say.

Joy L. Pritts, a health policy analyst at Georgetown University, said that in developing and promoting health information technology, the government seemed to assume that it could “tack on privacy protections later.” But she warned: “That attitude can really backfire. If you don’t have the trust of patients, they will withhold information and won’t take advantage of the new system.”

Executives can hire private tutors who specialize in teaching how to stay on the right side of the rules. But based on the experience so far, there is little chance that executives will be punished if they break them.

The Office for Civil Rights in the Department of Health and Human Services has received more than 22,000 complaints under the portability law since the federal privacy standards took effect in 2003; allegations of “impermissible disclosure” have been among the most common complaints. But the civil rights office has filed only three criminal cases and imposed no civil fines. Instead, it said, it has focused on educating violators about the law and encouraging them to obey it in the future.

With federal enforcement so weak, privacy advocates say they are also concerned about recent efforts in Congress to pre-empt state consumer protection laws. They often provide stronger privacy rights and remedies, particularly for information on H.I.V. infection, mental illness and other specific conditions.

State laws, unlike the federal law, have resulted in some stiff penalties. Last April, a California state appeals court approved a malpractice award of $291,000 to Nicholas Francies, a San Francisco restaurant manager, who lost his job after his doctor disclosed his H.I.V.-positive status in a worker’s compensation notice to Mr. Francies’s employer. He also got $160,000 from his employer in a settlement.

Dr. Deborah C. Peel, a psychiatrist and privacy advocate in Austin, Tex., has assembled a broad group called the Patient Privacy Rights Foundation, to lobby in Washington. Members span the political
spectrum, from the American Civil Liberties Union and the U.S. Public Interest Research Group to the American Conservative Union and the Family Research Council.

Newt Gingrich, the Republican former House speaker, has called for “a 21st-century intelligent health system” based on electronic records. He also says individuals “must have the ability to control who can access their personal health information.”

“People do have a legitimate right to control their records,” said Mr. Gingrich, who has worked closely with Senator Hillary Rodham Clinton, Democrat of New York, on the issue of computerized records. On their own, they have also advocated strict rules to protect privacy.

Mr. Gingrich noted that the Senate had twice passed bills to prohibit discrimination based on personal genetic information; the House did not vote on them. Democrats say the outlook for such legislation will improve when they take control of Congress.

EVEN without new federal laws to guide them, some companies have begun to encourage their employees to embrace electronic medical records. At Pitney Bowes, employees are paid a bonus if they store a copy of their personal health records on WebMD.com, the medical Web site.

“We haven’t pushed that, except to make an offering,” Dr. Pawlecki said. But for those without electronic records, he added, “any time you go to a different system or a different doctor, the chances are that your records will not be able to follow you.” As a result, there is a risk of “harmful care,” like drug interactions or side effects, he said, as well as risks of omitting needed care and conducting duplicate tests.

Pitney Bowes and WebMD Health are among a group of 25 companies meeting with Ms. Pearson of I.B.M. to develop a set of principles and best practices that she said would help persuade people that their employers really did not look at private information stored online.

Ms. Pearson’s group is working with Janlori Goldman, director of the Health Privacy Project in Washington. Employers need to adopt standards for personal health records that address their workers’ privacy, confidentiality and security concerns, Ms. Goldman said.

WebMD, which manages employees’ health records for dozens of companies, had discussions earlier this year with Google, which is developing a Web site called Google Health, according to people familiar with the project. Google has not commented on its plans. But commenting generally on the issues, Adam Bosworth, the vice president for engineering at Google, said that privacy is a hurdle for technology companies addressing health care problems.

“There is a huge potential for technology to improve health care and reduce its cost,” Mr. Bosworth said in a statement. “But companies that offer products and services must vigorously protect the privacy of users, or adoption of very useful new products and services will fail.”

Even before the theft this year of a Veterans Affairs official’s laptop that contained private medical records of 28 million people, a consumer survey found that repeated security breaches were raising concerns about the safety of personal health records.
About one in four people were aware of those earlier breaches, according to a national telephone survey of 1,000 adults last year for the California HealthCare Foundation. The margin of error was plus or minus 3 percentage points.

The survey, conducted by Forrester Research, also found that 52 percent were “very concerned” or “somewhat concerned” that insurance claims information might be used by an employer to limit their job opportunities.

The Markle survey, to be published this week, will report even greater worry — 56 percent were very concerned, 18 percent somewhat concerned — about abuse by employers. But despite their worries, the Markle respondents were eager to reap the benefits of Internet technology — for example, having easy access to their own health records.

Companies that have tried to use computers to increase the efficiency of medical care say their success has hinged on security. “The privacy piece was critical,” said Al Rapp, corporate health care manager at United Parcel Service, which recently introduced a health care program built on computerizing the records of 80,000 nonunion employees.

U.P.S. offers to add $50 each to workers’ flexible spending accounts if they agree to supply information for a personal “health risk appraisal.” They can receive another $50 if spouses also participate. More than half accepted, Mr. Rapp said, with the understanding that the information would go to data archives at UnitedHealth Group and Aetna. “We are not involved in any way,” he said, referring to U.P.S.’s managers.

Aetna and UnitedHealth combine these appraisals with each person’s history of medical claims and prescription drug purchases. When the software signals a personal potential for costly conditions like diabetes, heart problems and asthma, an insurance company nurse, or health coach, telephones the employee with suggestions for preventive care and reminders for checkups, taking medications and the like.

“The employee can tell the nurse who calls that they don’t want to participate,” Mr. Rapp said. “Thus far, it has been very well accepted.”

Last week, he said, the health coach reached out to the spouse of an employee after noting that her condition and weight suggested a potential risk for a heart attack.

“She asked this person, ‘Are you taking your cholesterol medication, Lipitor?’ She said, ‘I won’t take Lipitor,’ ” and went on to mention the side effects she had read about on the Internet, Mr. Rapp said.

The nurse informed the woman’s doctor, who changed her prescription to a similar drug, Mr. Rapp said. He added that he was one of “a very few select people in the human resources department” who are permitted to see personal health records, under the federal privacy rules.

“I can see the names, to see the issues,” Mr. Rapp said. “I manage the program. I have responsibility for the success of the program.” But he added that he was prohibited under the law from sharing the employee’s data with other U.P.S. managers. “Generally speaking, U.P.S. would have no knowledge of it,” Mr. Rapp said.
Still, worries linger across the health care system. Hospital executives say that private investigators have often tried to bribe hospital employees to obtain medical records that might be useful in court cases, including battles over child custody, divorce, property ownership and inheritance.

But computer technology — the same systems that disseminate data at the click of a mouse — can also enhance security.

Mr. Liss, of NewYork-Presbyterian, said that when unauthorized people tried to gain access to electronic medical records, hospital computers were programmed to ask them to explain why they were seeking the information.

Moreover, Mr. Liss said, the computer warns electronic intruders: “Be aware that your user ID and password have been captured.”