WISCONSIN'S MEDICAL BIG BROTHER

CHARLES J. SYKES

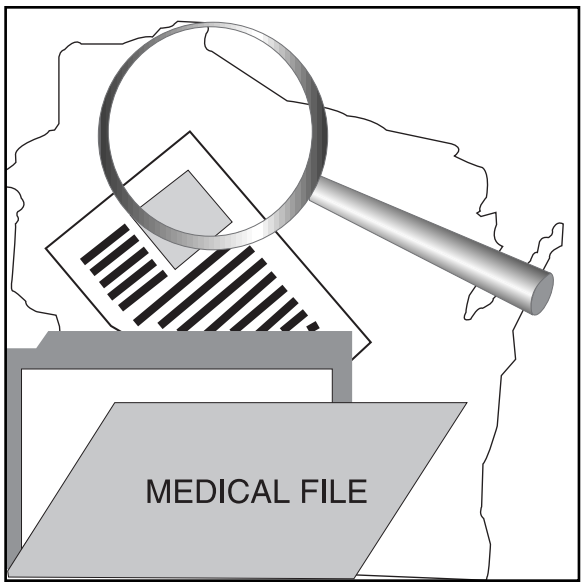
Hippocratic oath: Fifth century BC:

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about."

Hal Abbas (Ahwazi), advice to a physician, 10th century AD:

"A physician should respect confidences and protect the patient's secrets. In protecting a patient's secrets, he must be more insistent than the patient himself."

Geneva declaration, World Medical Association, 1940: "I will respect the secrets which are confided in me, even after the patient has died."



Despite the long tradition behind those principles, the State of Wisconsin regards doctor-patient confidentiality as obsolete, inconvenient, and since last year, illegal.

Last April, Governor Thompson signed into law a bill that requires doctors to report information to a new state databank about every patient visit, including the identities of their patients, their diagnosis, and their treatment. The bill was passed despite warnings that such a move not only intruded into doctor-patient relations, but was also a gross violation of medical privacy. Because the reports will be based on more than 13,000 diagnostic codes used by physicians, the information provided to state bureaucrats will be extraordinarily detailed.

The law also drastically expands the scope of state monitoring. Under the new rules more than 10,000 separate entities (up from 150 entities under old rules) will now be required to provide the state with once-confidential medical data. As a result of the legislation, the number of medical records submitted to state bureaucrats will rise from one million to *300 million.*

Moreover — and this is perhaps the most radical provision of Wisconsin's law — the state intends to release much of that information to the public, without ever asking patients for their permission or informing them that the state wants to know exactly what they are discussing with their doctors.

Charles J. Sykes *is the editor of* WI: Wisconsin Interest *and a senior fellow of the Wisconsin Policy Research Institute. He also hosts a talk-radio show on AM 620 WTMJ in Milwaukee. His most recent of four books is* Dumbing Down Our Kids: Why American Children Feel Good About Themselves, But Can't Read, Write, or Add, *published by St. Martin's Press.*

The State Medical Society fought hard against the measure, distributing fliers to patients reading:

> ALERT: This visit with your doctor will be reported to state bureaucrats without your permission. *The doctors warned*: The state should not have the right to know anything about your medical condition. It's your information about your health. Only you should have a say in whether your sensitive health information is sent to the state.

But the reporting measure was backed both by labor and business, which argued that the data would help them monitor the "health-care marketplace." One prominent business advocate insisted that the bill would help consumers "make better decisions about health-care purchases." Supporters insisted that it would be impossible for anyone to actually identify an individual patient from the information in the new state database. But the state's medical society pointed out that it would not necessarily take a computer hacker to identify a patient's medical records, because anyone could figure out the identity of a patient by looking at the information that is left on the insurance claim form that must now be submitted to the state. Because it is common practice for insurance companies to use Social Security numbers as their group number, it would take little effort to link the record to an individual patient. As if that were not easy enough, the federal government is still considering creating "universal patient identifiers," which would provide a nationwide link of all of a patient's files. With a universal identifier, all of the information from all of the databanks — both public and private — can be merged into a global dossier that traces every patient contact, every illness, and every drug, from birth until death.

In early 1999, legislation was introduced into the Wisconsin State legislature that would require that patients give their consent before medical information is released to the state. At a minimum, the push for patient consent will force Wisconsin to once again debate the issue of medical privacy.

Medicine and Privacy

If there is one area of life where most Americans expect privacy it is in their relationship with their doctors. A 1993 Louis Harris poll found that 96 percent of Americans thought that federal legislation should designate personal medical information as "sensitive" and impose penalties for its unauthorized disclosure. An equally overwhelming 96 percent said that it was important that individuals have the legal right to obtain a copy of their own medical records. In addition:

- 85 percent said that protecting the confidentiality of medical records was "absolutely essential" or "very important" in any health care reform.
- 75 percent said they were worried that medical information from a computerized national health information system would be used for many non-health purposes. More than a third (38 percent) were "very concerned."
- 60 percent believed that it was not acceptable for their medical data to be given to direct marketers by their pharmacists without their permission.
- 64 percent objected to medical researchers using their records for studies, unless they first got a patient's consent.

But while most patients believe that their relationship with their physician is confidential — analogous to their relationship with a priest or a lawyer — the reality is very different. No federal law protects the confidentiality of medical information or prevents its transfer, or even sale. In fact, no federal law even gives patients the right to see their *own* medical file. (While 34 states do have laws covering the confidentiality of medical records, only 28 give patients the right to review and correct their own files.)

A short list of those who might have access to a medical file would include HMOs, insurance companies, private and public databases, pharmacists, hospital workers, and employers. Especially in managed care, confidential medical information is shared with a startlingly wide range of providers including insurers, pharmacists, state health organizations,

researchers, employers, marketing firms, and pharmaceutical companies. The Medical Information Bureau in Boston maintains files on 15 million people who have applied for various kinds of insurance.

How does medicine reconcile this with the Hippocratic Oath?

"Hippocrates is 2,000 years old," says one executive of a managed care company. "Medicine isn't one-on-one anymore. It's a team effort."

In recent years, what had been a latent problem — society's casual approach to protecting medical privacy — has become an acute one, especially as those records are computerized and shared among linked databases across the country. New technology dramatically expands the potential for abuse, while the sensitivity of medical information — including the results of genetic testing and psychological treatment. "Data is like a prostitute," says one advocate for the mentally ill. "Once it's on the street, everybody has access to it." Not all of the threats to privacy come from illegal leaks of information. Much of the information that is disseminated is systematic; simply part of the routine that passes your medical information from file to file, where it can be scanned by dozens — or perhaps scores — of people.

The National Research Council has warned that the medical records of millions of Americans are vulnerable to abuse

The National Research Council has warned that the medical records of millions of Americans are vulnerable to abuse, noting that "today there are no strong incentives to safeguard patient information because patients, industry groups and government regulators aren't demanding protection." But the threats are very real. As medical care is increasingly provided in nontraditional settings — outside of hospitals and doctors' offices, patients often have medical records scattered among a number of providers. Not only are records routinely shared among dozens of individuals, such sharing is largely unregulated and often occurs not only without the consent of the patient, but usually without him or her even knowing that it is happening.

Even as the potential threat grows, the NRC panel found, there were few signs that anything will be done to protect medical privacy. Without a strong public outcry, there are few inducements either for politicians or medical providers to erect "firewalls" to prevent the wholesale leakage of medical data. Not only has privacy become collateral damage in the war against rising health costs, it is continually threatened by new technologies, government regulation, and professional acquiescence. Meanwhile science continues to race ahead of both law and medical ethics. There are some indications that anxieties over breaches of medical privacy may be creating a public health crisis as patients avoid treatment or the diagnosis of diseases and conditions for fear such information might could cost them jobs or insurance.

The State Dataweb

Despite the growing concern about the vulnerability of sensitive medical information, many politicians remain tone-deaf to the issue. Instead, in some states, government data banks monitor every time a patient is admitted to a hospital, is injured at work, gets a flu shot, has a sexually transmitted disease, or is considered at risk of delivering a baby prematurely. In Wisconsin, one study found at least 30 separate entities which collect and maintain personal medical data. (See sidebar.) Medicaid records are available for five years and law

The Wisconsin Medical Dataweb

State governments now routinely collect information about drug use and other behavioral information for worker's compensation and disability claims, research studies, protective placement, and registries that identify and track specific diseases. A study by the Data Privacy Project found that in Wisconsin, for example, no fewer than 30 separate entities collect and maintain personal health information that is either "identifiable or potentially identifiable." Moreover, such information was freely shared among a host of inside and outside agencies — released and re-released, used and reused, passed among dozens of entities without patients ever being told or asked for their consent.

In Wisconsin a *partial* list of medical databases maintained by state agencies included the:

- Breast and cervical cancer screening program
- Carpal Tunnel Syndrome program
- Childhood Lead Surveillance System
- Adult Blood Lead Level Evaluation and Surveillance
- Immunization Program
- Sexually Transmitted Diseases
- AIDS Prevention and Control program
- AIDS Drug Reimbursement Program
- AIDS Insurance program
- HIV Partner Notification Program
- Tuberculosis Prevention and Control Program
- Children with Special Care Needs Program
- Induced Abortion Reporting System
- Live Birth Records and Death Records
- Sensitive Death records
- Maternal and Child Health Reports and Data Analysis
- Resident-based Nursing Home Survey Data System
- Cancer Reporting System
- Chronic Diseases Program (such as renal disease and hemophilia)
- Wiscon Care Program, which provides primary health care services to low income participants.
- Data on confidential workers compensation and unemployment compensation claims, which may include information on illnesses, medical conditions and illnesses.

The state also keeps track of medical information maintained on adoptions, children in foster care and other individuals under supervision of the Division of Children and Family services; preadmission screening for the Bureau of Community Mental Health; ambulatory surgery data; inpatient discharge data; confidential medical information collected, reviewed and analyzed as part of providing crime victim service; data on disabled sportsmen who qualify for reduced recreational fees; occupational health information collected for OSIER; and health-related information collected on children with handicaps for special education services.

The survey found that 40 percent of the data collectors subcontract all or part of their responsibilities to outside parties. The State's Department of Health and Family services, for example, shares its health information with local hospitals, contract laboratories, researchers and so-called "utilization review" committees. The survey also found that the department also has "an electronic matching program with Northern Wisconsin Central Credit Union." Other information is shared with University of Wisconsin researchers. Medicaid information is freely shared with the Department of Justice and other law enforcement groups, while patient-identifiable data is shared with the federal centers for Disease Control, the National Center for Environmental Health, the Agency for Health Care Policy and Research, and the National Institute for Health. Confidential vocational rehabilitation information is shared with a wide range of state agencies, including child support collection agencies, as well as such federal agencies as the Veterans Administration and Social Security Administration.

Despite the rapid growth in the collection of data and the sophistication of the technology, few government agencies have kept pace, resulting in weak or lagging safeguards of the privacy of the information. Only a third of the health data systems were safeguarded with computer specifications tailored to their specific needs. The study found few restraints on mixing and matching, and merging this information among other governments or other state parties. Not only are there no extensive limitations on the reuse of patient data, the patients themselves are largely cut out of the process, because there are few chances for patients either to see their records or give their consent about the use of the information.

(Source: Carole M. Doeppers, "In the Balance: State Government and Medical Records Privacy," ACLU of Wisconsin Data Privacy Project, May 1998.)

enforcement officials do not even need a court order to inspect them.

But in a number of respects, Wisconsin's law goes farther. While most of the databases provide for government monitoring, Wisconsin's law is specifically designed to *release medical information to employers and the public.*

Every doctor and clinic in the state is required to send the state a copy of a health insurance form known as a "HCFA 1500." While the state will not release specific names or Social Security numbers, such information will be added and kept in the state's database.

But more troubling is the information that the state does release — information that could be used to identify individual patients and their medical treatment. Under Wisconsin's law, the state will release the city you live in, your specific medical condition, the cost of treatment, your zip code, your employer's name, and your age and gender. As a spokesman for the state Medical Society noted, "How tough would it be to put two and two together?" Moreover, the Society notes, the huge volume of new medical data sent to the state's dataweb "will vastly increase the chance of error, and possibly, attempts to identify patients."

Under the current law, patient consent is not required and there is no requirement that patients be informed that their information will be shared with state agencies

Under the current law, patient consent is not required and there is no requirement that patients even be informed that their information will be shared with state agencies, which in turn, may share it with their employers or the public. In April 1999, State Representative Scott Walker and other legislators proposed amending the medical reporting law to require patient consent before information is sent to the state bureaucracy. "If ever there were common sense legislation, this is it," said Dr. Jack Lockhart, the president of the State Medical Society of Wisconsin. "Here's what the whole debate boils down to. Who owns your health care information? The government — or you? You do, of course. And *you* should have control over who sees it."

The Politics of Privacy

But restoring patient confidentiality will not be easy. The reporting requirements continue to be strongly backed by a powerful anti-privacy coalition, including the state's major business groups and labor organizations. Both insist the data generated by the reporting is useful. A spokesman for Wisconsin Manufacturers & Commerce, for instance, insists that the reporting requirement will help employers monitor their health care costs more effectively. Terry Craney, president of the state's largest teacher's union, also enthusiastically backed the legislation because it would guarantee "access to information to ensure a wide range of quality health care options" and would make it easier for school districts to "achieve quality health care at a reduced price." Despite opposition from the State Medical Society and privacy advocates, it was supported by a bipartisan majority in the legislature and signed by Governor Thompson.

The breadth of the political support is striking, especially since it seems to fly in the face of overwhelming public sentiment. One statewide poll in late 1998 found that 82 of state residents opposed the requirement that physicians be compelled to provide the state with patient health care information; while 83 percent opposed letting employers have access to such medical data.

Apparently the public recognizes something that the politicians do not. Control over

medical information is the very essence of privacy. Even if doctor-patient information is useful, it is none of the state's business. Certainly, it could be argued that business and labor unions alike would find it highly useful to have the state supply them with detailed personal information about their customers or members, but usefulness is hardly a justification for violating basic rights.

The support of the business community is especially puzzling, given their usual opposition to government regulation and intrusion. Surely, they would not be as enthusiastic about a government database that monitored every contact between a business and its customers, although undoubtedly some special interest group might find such information both advantageous and edifying.

Perhaps even more remarkably, a Republican legislature and Republican governor seem to have forgotten that most of their voters want less government, not more. Yet, they backed an extraordinary expansion of government surveillance and authority. That Republicans chose to create the dataweb at the behest of outside interest groups hardly makes the decision more palatable. Indeed, it raises fundamental questions not only about the policy, but also the constitutionality of the state's medical Big Brother.

Privacy and the Law

The U.S Supreme Court has recognized two distinct forms of the constitutionally protected right to privacy. The first is the right to make fundamental personal decisions, including choices about sexuality and reproduction. But the court has also found that the constitution also protected "the individual interest in avoiding disclosure of personal matters...." Significantly, the Court declared the existence of a constitutional right to informational privacy in a case upholding New York's centralized drug database — which tracked patients by name.

In the mid-1970s, New York State passed a law requiring physicians to identify patients obtaining certain kinds of prescription drugs for inclusion in a statewide database run by the state's Department of Health. Specifically, the database would track prescriptions of so-called Schedule II drugs — narcotics which were legal but had a potential for abuse. The database would include the names of the doctors, as well as the patient's name, address, age, and drug dosage. Under New York's law, the records would be kept in strict confidence and destroyed after five years and public disclosure was limited to a small number of health department employees and investigators.

Initially, a three judge District Court blocked the system, ruling that the doctor-patient relation was one of the zones of privacy protected by the constitution. The law's requirement that doctors report information about their patients to the state, the judges ruled, invaded that private zone with "a needlessly broad sweep." But when the U.S. Supreme Court considered the case, known as *Whalen v. Roe*, the justices were unanimous in upholding the legality of the medical database along with its reporting requirements.

Essentially, the high court ruled that a centralized database like New York's did indeed pose a threat to privacy, but that under the circumstances, New York's specific plan did not violate the constitution.

It is far from clear that the Court would take so benign a view of Wisconsin's database. Unlike New York's, Wisconsin's is not limited to a single category of medication — it is a global-medical database that includes every conditions, disease, treatment and medication offered. Even more problematical, however, are Wisconsin's provisions for releasing medical information to the public and the danger that the medical privacy of individuals will be violated.

One additional possible avenue for constitutional challenge is suggested in a related case known as *Department of Justice et al; v. Reporters Committee for Freedom of the Press,* in which the Court limited the power of government to release personal information to the media or the public. The case involved a request by reporters for the "rap sheet" of a man named Charles Medico. The media won in the Court of Appeals. But in a dissent, Judge Kenneth

Starr (who would later become the independent counsel who would plague President Clinton) wrote that the use of computerized data banks had changed the privacy landscape.

> We are now informed that many federal agencies collect items of information on individuals that are ostensible matters of public record. For example, Veterans Administration and Social Security records include birth certificates, marriage licenses, and divorce decrees (which may recite findings of fault); the Department of Housing and Urban Development maintains data on millions of home mortgages that are presumably 'public records' at county clerks' offices....

If the courts upheld the reporters' request for the federal printouts of such records, Starr warned, the "federal government is thereby transformed in one fell swoop into the clearinghouse for highly personal information, releasing records on any person, to any requester, for any purpose." This is not at all what Congress had in mind. The Freedom of Information Act was designed to keep government honest; it was not designed to turn it into the ultimate gatherer and disseminator of information about private citizens. The law was designed to open windows onto the government, not turn the government into a microscope.

The Supreme Court agreed with Starr. The Court not only reiterated the constitutional right to informational privacy, but by balancing the need for transparency and accountability with the need to keep government from becoming surrogate snoop, it had also established a useful guideline for resolving other disputes about open records and privacy. Government, it argued, can be kept accountable, without turning it into an instrument of surveillance of fellow citizens. If this principle could be applied to an individual's criminal record, why would it not be equally applicable to far more private medical information?

While it may be difficult as a practical matter to regulate private information brokers and marketers, the Court has set out the constitutional parameters for sharply limiting both the government's information gathering abilities and its right to disseminate such personal information to others. This could be helpful in any attempt to scale back, limit, or abolish the many government databases, which threaten to undermine personal privacy. At minimum, such databases should be limited to using personal information strictly and exclusively for the purpose for which it was gathered.

Wisconsin's medical reporting law fails that basic test at every point: it uses the power of the government to allow third parties to monitor the behavior of private citizens.

It is bad policy, bad politics, and possibly unconstitutional.