



SCHOOL OF LAW
CASE WESTERN RESERVE
UNIVERSITY

Health Matrix: The Journal of Law-
Medicine

Volume 8 | Issue 2

1998

SCHROEDER SCHOLAR-IN-RESIDENCE LECTURE -- Health Care Information and Privacy

Donna E. Shalala

Follow this and additional works at: <https://scholarlycommons.law.case.edu/healthmatrix>



Part of the [Health Law and Policy Commons](#)

Recommended Citation

Donna E. Shalala, *SCHROEDER SCHOLAR-IN-RESIDENCE LECTURE -- Health Care Information and Privacy*, 8 Health Matrix 223 (1998)

Available at: <https://scholarlycommons.law.case.edu/healthmatrix/vol8/iss2/8>

This Article is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Health Matrix: The Journal of Law-Medicine by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.

SCHROEDER SCHOLAR-IN-RESIDENCE LECTURE

HEALTH CARE INFORMATION AND PRIVACY†

Donna E. Shalala††

FOR ME, THIS IS A MOMENT when the past and future meet. I have come home to Cleveland to speak at a university that has always been a leader in the future of health care.

In 1970, our nominee for Surgeon General, Dr. David Satcher, became the first African-American student here to earn simultaneous M.D. and Ph.D. degrees. And as you well know, in 1948, Professor Oliver Schroeder founded the first program for law and medicine in our nation.

Now, almost fifty years later, I am truly honored to join the ranks of the distinguished thinkers who have given the lecture dedicated to the vision and commitment of this extraordinary leader.

It is only fitting that I have come here today to talk about one of the most serious issues facing our health care system; something that affects every single American – every single one of you. That is the privacy of our most cherished and personal information: our medical records; our family secrets.

Until recently, at a Boston-based HMO, every single clinical employee could tap into the computer records of all its patients and see detailed notes from psycho-therapy sessions. In Colorado, a medical student copied countless health records at night and sold them to medical malpractice attorneys looking to win easy cases. And, in a major American city, a local newspaper published information about a Congressional candidate's attempted suicide; information she thought was safe

† Secretary Shalala spoke extemporaneously. This text is the basis of her oral remarks.

†† United States Secretary of Health and Human Services.

and private at a local hospital. She was wrong.

What about us? When we give a physician or health insurance company precious information about our mood or motherhood, money or medication, what happens to it? As it zips from computer to computer, from doctor to insurance company to hospital, who can see it? Who protects it? What happens if they do not protect it? It all depends on the state in which you live.

Every day, our private health information is being shared, collected, analyzed, and stored with fewer federal safeguards than our video store records. That is important. We have federal laws that protect the privacy of our video records, our motor vehicle records, and our credit records. But, the way we protect the privacy of our medical records right now is erratic at best – dangerous at worst.

I will argue today that, to eliminate this danger to our citizens and our health care system, we must act now with national legislation, national education, and a national conversation.

As I was preparing this speech, I thought about a similar challenge faced by one of my predecessors, Secretary Elliot Richardson. The year was 1972 – twenty-five years ago. America's military involvement in the Vietnam War was coming to a close, and the first chapters of Watergate were being written. Public distrust of government was on the rise. And the computer age was just beginning.

It was against this backdrop that Secretary Richardson appointed an advisory committee to help the government figure out how to protect the privacy of data in this new world of technology. The report outlined a code of fair information practices, including the need to eliminate secret data bases and give people more control over their personal information. It built the foundation for the landmark Federal Privacy Act which protects the privacy of records kept by federal agencies. And, it helped lay out a vision for balancing our age-old right to be left alone with our desire to fulfill the promises of a new computer age.

That is what we must do today – this time for our private health records. It is also what we, as nations and individuals, have always struggled to do. DeToqueville described how our

Founding Fathers dealt with the tension between individual rights and public responsibilities. Great Americans like the late Justice Brennan dedicated themselves to protecting the individual against an all too powerful government and majority. Books like *1984*¹ sent a warning about lost autonomy – and lost humanity. Throughout time, individuals have grappled with privacy, whether they are getting an HIV test at a local clinic or complaining, as they did recently, about America Online's plan to sell its mailing list.

Yet, while our desire to be left alone has always remained constant, little else has done so. A lot has changed since Secretary Richardson confronted this issue. Twenty-five years ago, our health care privacy was protected by our family doctor who kept hand-written records about us sealed away in a big file cabinet. We trusted our physicians to keep their file cabinets locked and their mouths shut. We trusted them not only because of the Hippocratic Oath and the fundamental ethics of medicine, but because we knew them. They took care of our entire families. We asked their advice about our personal problems. We went to school with their children. We shopped at the same stores. They came over for dinner – and yes, some even made house calls.

Today, the revolution in our health care delivery system means that instead of *Marcus Welby*,² we have to place our trust in entire networks of insurers and health care professionals – both public and private.

The computer revolution means that our deepest and darkest secrets no longer exist in one place and can no longer be protected by simply locking up the office doors each night. And, revolutions in biology mean that a whole new world of genetic tests have the potential to either help prevent disease or reveal our families' most personal secrets. Because without safeguards protecting citizens from being endangered by genetic testing, perhaps endangering their families' privacy, or health insurance or jobs, we could, in turn, endanger one of the most promising areas of research our nation has ever seen.

We are at a decision point. Depending on what we do

1. GEORGE ORWELL, *1984* (1983).

2. Marcus Welby, M.D. (NBC television broadcast, 1968).

over the next months, these revolutions in health care, communications, and biology could bring us great promise or even greater peril. The choice is ours.

We must ask ourselves: Will we harness these revolutions to improve – not impede – our health care? Will we harness them to safeguard – not sacrifice – our privacy? And will we harness these revolutions to strengthen – not strain – the very lifeblood of our health care system – the bond of trust between a patient and doctor.

For example, will health care information flow safely to improve care, cut fraud, ensure quality, foster research, and reach citizens in underserved areas? Or will it flow recklessly into the wrong hands – and be used to deny our citizens health insurance, jobs, and the confidentiality they expect and deserve? It is up to us.

The Institute of Medicine has said that electronic health records should be the wave of the future, and the Congress has asked us to develop standards to make it happen. Will they be used to help an emergency room doctor learn more about an unconscious patient – alerting him to what diseases she has and which medications she is allergic to? Will it be used – as it can be now – to tell parents which immunizations their children have – and which ones they still need? Or will a pharmaceutical company use it to market the newest anti-depressant to someone with a family history of depression? Will a political group use it to embarrass a rival they believe once had an abortion or a child with a drug problem?

The fundamental question before us is: Will our health records be used to heal us or reveal us? The American people want to know. And, as a nation, we must decide.

Today, almost seventy-five percent of our people say that they are at least somewhat concerned that computerized medical records will have a negative effect on their privacy. In one survey, about one-fourth of adolescents say they would not seek medical care unless their privacy and confidentiality were protected. And, how many people do you know – do all of us know – who have insurance but often choose not to use it because they are afraid someone will find out about their therapy or other sensitive care?

If we do not act now, public distrust could deepen and

ultimately stop citizens from disclosing vital information to their doctors, getting needed treatment for mental illness, going in for genetic tests, and participating in clinical research trials. We have already seen this happen with some groups in the aftermath of the experiments at Tuskegee. And we know that, if unchecked, distrust can undermine and stop progress in our entire health care system.

The question is, what can we do? There are some who say we have already lost the battle. They say privacy in this new electronic world is impossible. Just give it up. Then there are others who say that consumers should not only have control over their health care information. They should have complete control. They say that Americans should even have the power to ensure that their records are kept on paper, not in computers. Both of these approaches are wrong. We cannot turn back the hands of progress or turn our backs on public responsibilities like research – and we should not. But we can and must do what Secretary Richardson envisioned: to look ahead and safeguard privacy in this new world of progress. Health care privacy can be safeguarded. To do that, we must, first and foremost, enact national legislation to protect the privacy our medical records and we must do it now. As I have said, we have federal laws that protect the privacy of video records, motor vehicle records, and credit records. But, when it comes to our private health care records that can reveal personality traits, Sexually Transmitted Diseases, and depression; when it comes to personal information that travels in real time across hospitals, doctors' offices, and state lines – even international borders, we rely on a patchwork of state laws. The fact is, we have no real federal health care privacy standards. We have no national standards. We do have a national interest – now we must make a national commitment. Congress asked our Department to make recommendations regarding the Kassebaum-Kennedy law.³ These recommendations to Congress are guided by five key principles.

First, the principle of boundaries. With very few exceptions, a health care consumer's personal information should be

3. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

disclosed for health care and health care only. We want to make it easier to use information for health care purposes and very tough to use it for any other purpose. For example, we recommend that a hospital be able to use personal health information to teach, train, conduct research, provide care, and ensure quality. But on the other hand, employers who get health care information to pay claims cannot use it for any non-health purposes – like hiring, firing, and promotions.

And, what about the third parties; those who more and more often are hired to do billing and other services? They must be bound by the same tough standards. Even if they do not collect it, they still must protect it.

Second, there is the principle of security. When Americans give out their personal health care information, they should feel like they are leaving it in good safe hands. Think about all the ways that private information like your genetic tests could become public. People who are allowed to see it – like those at the lab – can misuse it either carelessly or intentionally. And, people who should not be seeing it – like marketers – can find a way to do so anyway – either because an organization does not have proper safeguards or they find an easy way around them.

If we are going to block this leakage, Congress must pass a law that ensures that your personal health information will not be given out unless you authorize it, or if there is a clear legal basis for doing so. Moreover, legislation should require those who legally receive health information to take real steps to safeguard it. That means they must ensure that it is not used improperly by those who have access to it, and it is not obtained improperly by hackers or others on the outside.

Third, we must deal with the Principle of Consumer Control. Americans should not have to trade in their privacy rights to get quality health care. We believe that citizens should be given clear explanations of how organizations will use their records – and what their rights are if this information is misused. They should have the power to find out who is looking in their records; what is in them; and how to inspect, copy, and if necessary, correct them.

Let me give you an example of why this is important. According to the Privacy Rights Clearinghouse, a physician in

private practice was having trouble getting health disability and life insurance. She ordered a copy of her report from the Medical Information Bureau – a clearinghouse used by many insurance companies. It included information about her heart problems and her Alzheimer's disease. There was only one problem. None of it was true. What if she had not requested her records? With electronic data, mistakes can multiply – and sunlight is still the best disinfectant.

Fourth, we need to address the principle of accountability. If you are using or obtaining information improperly, you should be severely punished. And if you have been entrusted with using information, you must be accountable for its misuse. For example, we cannot just tell a hospital worker to stay away from private medical records. We cannot just tell a private investigator not to lie about their identity in order to see a patient's records. We need to enforce our messages with real criminal penalties for those who misuse personal information and real civil redress for those who have been harmed by its misuse.

At the same time, our nation needs to address another legal issue that has a tremendous impact on how people view their privacy: health care discrimination. For some, the privacy issue did not really catch their eye until the AIDS epidemic unfolded. Remember the outrage that occurred when someone leaked a list of people with AIDS from a public health clinic in Florida? With AIDS, citizens do not just have to worry that people will know they are sick. They also have to worry that people will make assumptions about their sexual orientations – and use that information or their health status to discriminate against them.

The fact is, we will never fully address the issue of health care privacy until we give all Americans confidence that information in their medical records will not be used to deny them jobs or affordable health insurance. That is why the Kassebaum-Kennedy law says you cannot deny someone health insurance just because they have a pre-existing condition. And it is why the President recently announced his support for Congresswoman Slaughter's proposal to wipe-out genetic discrimination in health insurance.

But, these four principles – boundaries, security, consumer

control, and accountability – must be weighed against another – yet sometimes competing – fifth principle, Public Responsibility.

Just like our free speech rights, privacy rights can never be absolute. We must balance our protections of privacy with our public responsibility to support national priorities – like public health, research, quality care, and our fight against health care fraud and abuse.

For example, public health agencies use health records to warn us of outbreaks of emerging infectious diseases. Researchers have used health records to help us fight childhood leukemia and uncover the link between DES⁴ and reproductive cancers. And auditors use health records to zero in on kick-backs, over-payments, and other fraud – so we can bring the perpetrators to justice and the money back to the taxpayers. In fact, over the past four years our overall anti-fraud efforts have increased the number of health care fraud convictions by 240%, saving taxpayers more than \$20 billion.

In all of these cases, it is not always possible to ask for permission. And, in many cases, doing so could create major obstacles in our efforts to fight crime and protect public health. But, that does not give us a free pass. Allowing access does not mean that we can forget about protecting privacy. And we should not. Take the case of research. We already rely upon institutional review boards to limit access to personal information and determine if it is necessary and advisable to waive the normal informed consent required to use medical records. Our new recommendations go even further. They will make it clear that all researchers must carefully protect the privacy of the personal information they receive – and we recommend penalties if they do not. That is important. If we do not protect health records soon, we may no longer be able to trade valuable research data with Europe, under the new Privacy Directive of the European Union (E.U.). And, as Dr. William Lowrance made clear in a recent report I requested, if people do not trust the research community to protect their personal information, they may refuse to participate in clinical trials and

4. Diethylstilbestrol (DES) is a synthetic form of estrogen used in the 1940s and 1950s to prevent miscarriage during pregnancy.

they may even oppose the use of their records for all research – no matter what the circumstances. That could be devastating.

Because there has been some confusion, I also want to make our position on law enforcement access very clear. Despite press reports to the contrary, we are not recommending any changes to existing laws that govern how law enforcement officials get or use health care information. But, we are recommending – and this is important – new penalties for law enforcement officers and others who misuse the personal health care information or get it under false pretenses. And we are recommending that people whose health care information is misused by law enforcement officers should be able to seek civil action for damages.

We believe we have succeeded in striking the right balance between giving our law enforcement officials the tools they need to protect our citizens from crime and giving our citizens the safeguards they need to protect them from breaches of confidentiality.

But, national standards alone will not inspire trust in one's rights or commitment to one's responsibilities. We need a major commitment to education. Every single health care professional, every insurance agent, every researcher, every member of an IRB, every public health official, every pharmacist, and, yes, every member of the press – every single person who comes in contact with health care records must understand why its important to keep them safe, how they can keep them safe, what will happen to them if they do not keep them safe.

And we need to enlist their help – your help – in educating all consumers not just about their privacy rights, but also their responsibilities to ask questions and demand answers – to become active participants in their health care.

We need an informed public – because, as the National Research Council recently pointed out, we need an informed public debate; a national conversation to answer the tough questions as they arise. This is my final point.

These questions will sometimes be wrenching. They will always be changing. But, they are not going away. We cannot expect to solve this problem all at once. We need to be flexible, to change course if our strategy is not working and meet new challenges as they arise.

When the Human Genome Project was created, we did not know what miracles it would uncover. But, we did know we needed to devote real resources and energy to examine the legal, ethical, and social implications of all that we find, so that our ethics would always be just as sophisticated as our science. This is so that, as Jefferson said, and I paraphrase, our laws and institutions would always keep pace with the human mind.

Twenty-five years ago, Secretary Richardson looked into an uncertain future and tried to chart a course where individual rights and privacy would prevail. That challenge is now before us. Twenty-five years from now, what will they say about the footprints we left? Will we leave the next generation with real federal privacy standards based on fundamental principles? Will we have boundaries to ensure that our health care information is used only for health care? Will we have assurances that our information is secure? Will we have control over what happens to it? Will those who violate our privacy be held accountable? And, will we be able to safeguard our privacy rights while still protecting our core public responsibilities such as research and public health?

In short, will we harness these revolutions in biology, communications, and health care to breathe new life into the trust between our patients and their doctors, between our citizens and their government, between our past and our future?

We can. We must. And, if we act today, we will.